BDO IN SOUTH AFRICA | FINANCIAL SERVICES

INTRODUCTION TO THE INTERNET OF THINGS

AUDIT • ADVISORY • TAX

TABLE OF CONTENTS

A BRAVE NEW WORLD: A SHORT INTRODUCTION TO THE INTERNET OF THINGS AND ITS EFFECTS ON SOCIAL ENGINEERING

Christopher James O'Flaherty
BDO Financial Services Technology Junior Analyst

The exponential growth of technology, leading to the fourth industrial revolution, encompasses a variety of new emerging technologies changing life as we know it on a day to day basis (World Economic Forum, 2020).

The Internet of Things (IoT), Quantum Computing, Blockchain and Artificial intelligence are few of the many technologies shaping the future of how business is conducted in the modern world (TechRepublic, 2020). This paper explores IoT and its development in recent years which has led to the creation of financial opportunities, along with a multitude of security threats. IoT encompasses technology embedded into a multitude of items, including household (every day) items, which enable connectivity between these items, and the internet. The devices are assigned an IP address and functionality is enhanced. Responsive devices include, but are not limited to, cars; thermostats; security systems; appliances, such as toasters and fridges; lights; alarm clocks and vending machines (Elon.edu, 2020).

The table below represents the rapid growth of IoT over the last seven years with predictions for 2020 being over eight times greater than in 2013.

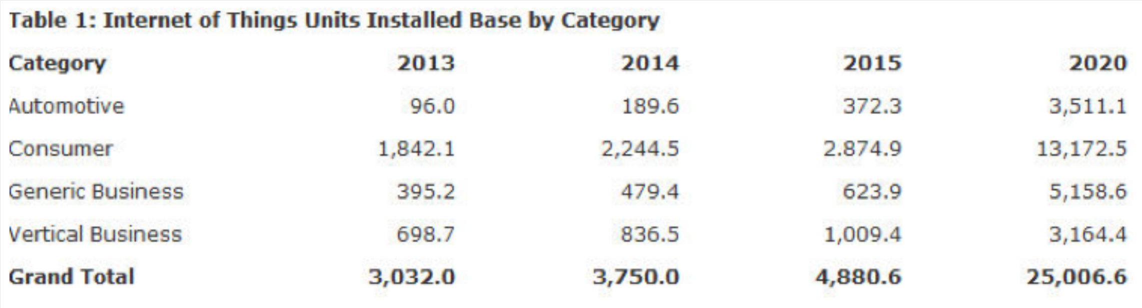


Table 1: Internet of Things Units Installed Base by Category

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

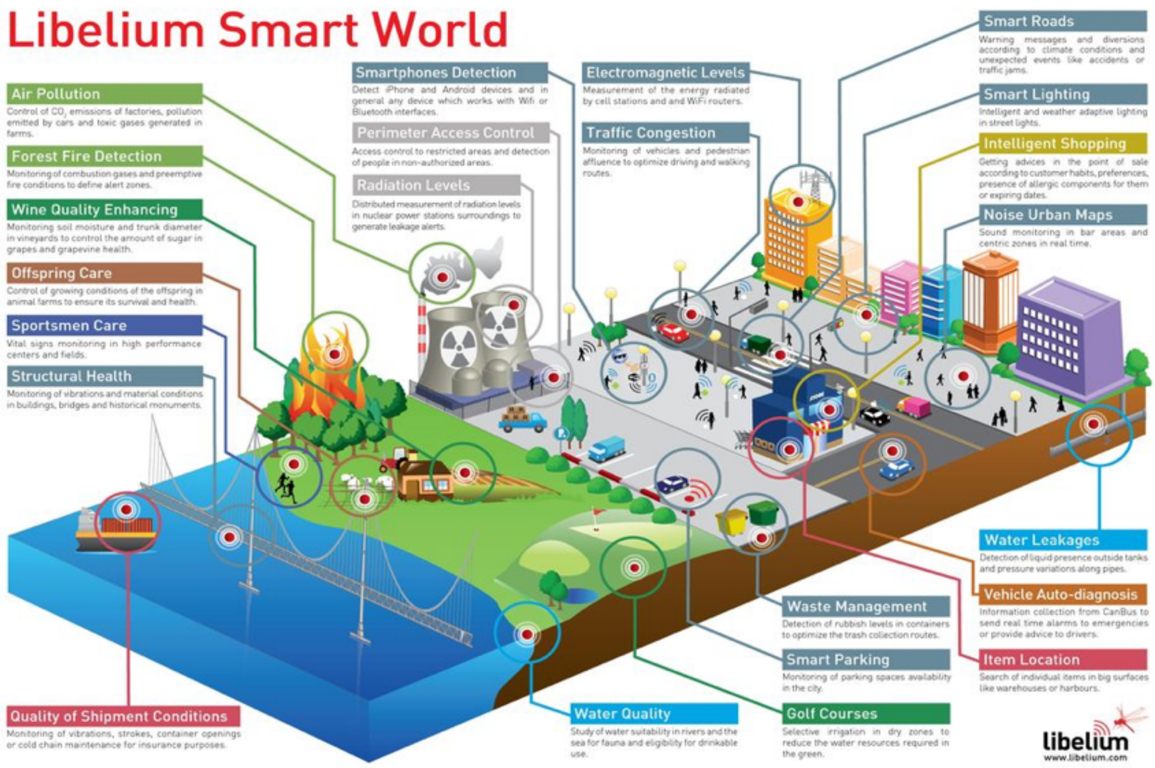
Figure 1: Source: Gartner Inc

Owing to the growth of emerging technology, over nine billion devices are currently connected to the internet, with Gartner expecting it to rise to over 20 Billion in 2020 (Muddana, 2020). The growth of technology has resulted in changes to everyday life through automation and artificial intelligence. From the above table, we can see how the number of IoT devices has exponentially increased. IoT has made many everyday activities far easier and convenient. A smart fridge can order your food when supply is low and a smart kettle can boil water daily at a specified time (Midrack, 2019). IoT incorporates device collaboration. When travelling to a meeting, your car may have access to your calendar and if there is heavy traffic, it can alert the person who is to be met that you may be late. This incorporates GPS, as well as your device and calendar which will alert another user (Houkom, 2018).

A BRAVE NEW WORLD
THE LIBELIUM SMART WORLD
IOT AND FINANCE
IOT AND SECURITY
SOCIAL ENGINEERING
IOT AND BIG DATA
THE EFFECT ON ORGANISATIONS
AN AUDIT APPROACH
DEFENCE MECHANISMS
CONCLUSION
REFERENCE LIST

THE LIBELIUM SMART WORLD:

According to Libelium, the Spanish platform provider for the Internet of Things believes that IoT can improve our daily lives in a myriad of ways and says with the Fourth Industrial Revolution on our doorstep, its concept of a smart world is close to coming to fruition. Below is a picture of what this world entails:



Libelium Smart World

Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Sportsmen Care
Vital signs monitoring in high performance centers and fields.

Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.

Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.

Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Electromagnetic Levels
Measurement of the energy radiated by cell stations and and WiFi routers.

Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.

Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Smart Lighting
Intelligent and weather adaptive lighting in street lights.

Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.

Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.

Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.

Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.

Smart Parking
Monitoring of parking spaces availability in the city.

Item Location
Search of individual items in big surfaces like warehouses or harbours.

Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.

Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

Figure 2: The Libelium Smart World

The Libelium Smart World depicts how sensors will enhance the world as we know it. It encompasses smart cities, including smart parking systems allowing drivers to detect a parking in the nearby vicinity. Structural health will assist in the monitoring of vibrations and conditions of buildings and infrastructure. Smartphone detection, traffic congestion assistance, smart lighting and smart waste management are all examples of how smart cities have started to function. Moreover, the Libelium Smart World also focuses on a smart environment; smart water; smart metering and security and emergencies.

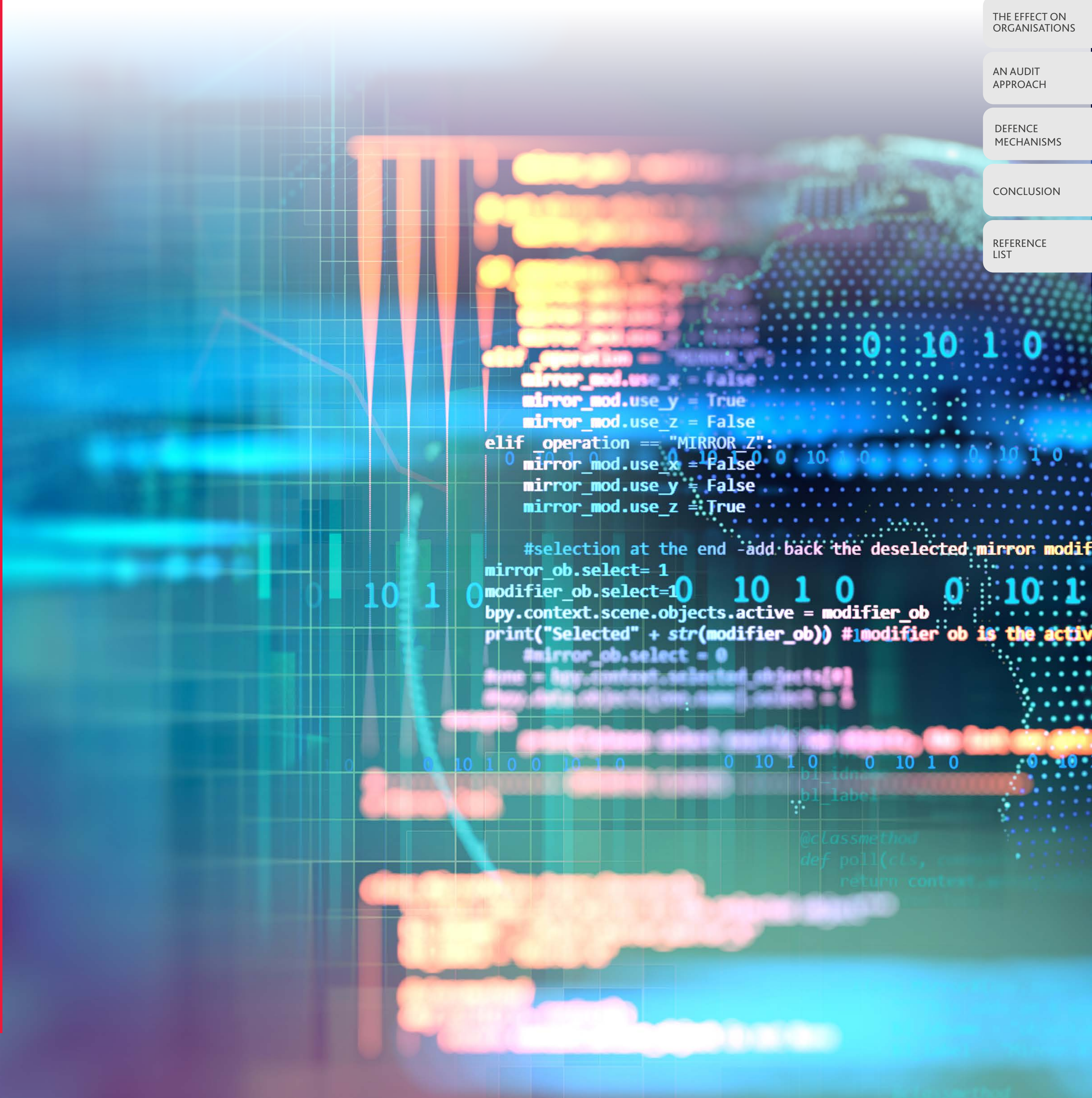
The smart environment will include fire detection, air pollution control, snow level monitoring, landslide and avalanche prevention as well as early earthquake detection. Sensors will detect certain anomalies and alert a system when issues arise. The issues can then be mitigated through early detection. Smart water will include potable water monitoring, chemical leakage detection in rivers, swimming pool remote measurement, pollution levels in the sea, water leakages and river floods. Smart metering will include a smart grid, the monitoring of tank levels, photovoltaic installations, water flow measurement and silos' stock calculation. Potentially you could be able to monitor all power usage in one's home, turning off switches via mobile devices along with various other uses. Finally, the smart world will have extensive measures for security and emergencies including perimeter access control, a detection system for liquid, radiation monitors and a detection for explosive and hazardous gases. All these will be highly effective in industrial settings (Libelium, 2020).

IOT AND FINANCE:

The advent of the Fourth Industrial Revolution has created a multitude of financial opportunities and business ventures. A recent example includes the purchase of company “Fitbit” by Google for $2.1 billion (Wakabayashi and Satariano, 2019). Usage-based insurance policies may also disrupt the financial and insurance sector with new policies being introduced. Devices are able to monitor a person’s health, wellbeing, what they do on a day to day basis and various other specifics. Through the access and use of this data, companies can adjust their policies to ensure a complex usage-based approach (Newman, 2020).

Building construction and various other industrial methods have been disrupted through IoT. Drones are now able to capture a building site and estimate its value and cost to completion. "In simple terms, the IoT is just a new source of data acquisition and a mechanism to enable the control of physical objects remotely. However, the indirect impact will be disruption in markets where uncertainty about the future plays a significant role" (How the Internet of Things will change finance, 2019).

A BRAVE NEW WORLD
THE LIBELIUM SMART WORLD
IOT AND FINANCE
IOT AND SECURITY
SOCIAL ENGINEERING
IOT AND BIG DATA
THE EFFECT ON ORGANISATIONS
AN AUDIT APPROACH
DEFENCE MECHANISMS
CONCLUSION
REFERENCE LIST


mirror_mod.use_y = True
mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modif
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the activ
10 1 0

IOT AND SECURITY:

But with great power comes great responsibility. Security is of the utmost importance owing to the fact that if one node in this system were to be tampered with, it would affect various others. A decentralised system including block chain tendencies would assist in this regard (Miles and Miles, 2017).

One needs to be aware that if a hacker to gain access, he may be able to tamper with all of one's devices. Security on smart homeware is usually fairly basic owing to the fact that companies race to get products to market and only worry about security concerns later (Entrepreneur Council, 2018). These devices also collect and store vast amounts of data. This data can be attractive to hackers enforcing the need for security measures.

Below are a few interesting cases regarding the implementation of IoT:

- IoT data has spread as far as electronic chips being implanted into cows' ears to monitor their health and their activities creating approximately 200mb of data per cow per annum (Evans, 2011).
- As specified earlier, when travelling to a meeting your car may have access to your calendar so it can calculate the best route for you to travel and also notify a client if there is a lot of traffic and that you are going to be late (Houkom, 2018).
- Your alarm clock can connect to your coffee machine wherein coffee will start brewing as your alarm goes off (Midrack, 2019).
- If you are low on supplies in the fridge, or the office, your device could order more stock from an online retailer (Midrack, 2019).

Owing to the fact that these devices are connected, they could be manipulated and leave one vulnerable, causing you to worry whether:

- Will someone be able to hack into your toaster and thereby get access to entire network?
- Will your privacy and data be accessed by the companies providing these services, and if so, do you mind?
- The mass of devices will collect, store and analyse a large amount of data which needs to be stored securely from malicious attackers.
- Producers may try to get a product to market quicker rather than focus on security concerns. Is it better to therefore rather wait for a second-generation product? (Entrepreneur Council, 2018)
- Industry accepted standards are few and far between the variety of security frameworks set by industry leaders. Should regulations be set for this? (Hajdarbegovic, 2020)
- The variety of standards make it difficult to secure systems as well as to ensure interoperability between them (Rouse, 2020).
- IT (Information technology) and OT (Operational Technology) have converged creating security challenges necessitating a sharp learning curve for those involved in the development of these devices (Rouse, 2020).

The threat landscape is thus magnified. An example of a recent security breach concerns a baby monitor being hacked and a stranger communicating through it to somebody’s child (Ngak, 2013). Moreover, in 2015, security researchers Charlie Miller and Chris Valasek executed a wireless hack on a Jeep. They changed the radio station on the car's media center while also turning its windshield wipers and air conditioner on. They were able to stop the accelerator from working. They said they could stop the engine, engage the brakes and disable the brakes. Miller and Valasek were able to infiltrate the car's network through Chrysler's in-vehicle connectivity system, Uconnect (Greenberg, 2015). If systems like this are hacked on a mass level, the devastation that would occur would be monumental with various car accidents, deaths and destruction of infrastructure.

Companies strive to evolve with the revolution. Legacy assets are assets which have been used for many years and have thus depreciated to a zero value. These assets occasionally perform roles which can be fairly difficult to upgrade or change. A mainframe at a bank is a clear example. If this were to be tampered with, or upgraded, it may be fairly expensive to do, as well as complex. In recent times, attempts have been made to upgrade legacy devices which have the potential to leave the device susceptible to new attacks and threats. Corporations should bear this in mind when upgrading these systems (Behrtech Blog, 2019).

SOCIAL ENGINEERING:

“Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain” (Rouse, 2020).

Through the use of social engineering, combined with the various vulnerabilities incorporated with emerging IoT, the threat landscape has exponentially increased in a multitude of sectors. Social engineering was performed primarily through email and website platforms however vehicles, home appliances and numerous other devices and tools are now susceptible. Naïve users and simple passwords result in easy access for attackers and leaves one to wonder how future-proof passwords are (Hoenes, 2019). Damage to manufacturing plants, train and tram signaling, and nuclear power plants have been caused by such attacks. A malicious computer worm, Stuxnet, caused substantial damage to the nuclear program of Iran (Camacho, 2013). Further examples include:

- In December 2014, a German steel mill furnace sustained damage when hackers used targeted phishing emails to capture user credentials, thereby gaining access to the back office and ultimately the production network (Hartfield and Gan, 2016). With this access, infiltrators could perform various tasks and drastically influence the business.

- Another example is when households in Ukraine suffered a blackout on 23 December 2015 caused by an attack that brought down the power grid. The attackers used phishing emails to trick users at the electric company into clicking on an attachment in an email, ostensibly from the prime minister of Ukraine. This is thought to be the first cyber-attack that brought down an entire power grid, leaving 225,000 homes without electricity (Hartfield and Gan, 2016).

- In extreme circumstances, attackers may even begin to target medical devices (e.g., pacemakers or mechanical insulin-delivering syringes) via near-field communications or wireless sensor networks, in an approach analogous to ransomware. This has already occurred through the IoT using conventional hacking techniques (i.e., SSH vulnerabilities and unpatched systems with default hardwired passwords) and is commonly known as a MEDIJACK attack (Hartfield and Gan, 2016).

IOT AND BIG DATA:

Big data is a common term describing large amounts of data. Companies such as Dawex (Sell, buy and share data, 2020) buy and sell data and have various uses for this data whether it be to make strategic business moves, or to understand a clientele. Owing to this, data is an attractive object and large amounts of it is created by the numerous IoT devices. There are now more ways for hackers to reveal information about people and there is growing amount of information to steal. Hackers can access people's day to day activities ranging from where they have gone, what time they have their morning coffee and who their family members are. This results in crimes including, but not limited to, identity theft and information theft.

There are multiple methods of social engineering. Common forms of social engineering include the following:

- "Baiting: Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive, in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.
- Phishing: Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.
- Spear phishing: Spear phishing is like phishing but tailored for a specific individual or organisation.
- Vishing: Vishing is also known as voice phishing, and it's the use of social engineering over the phone to gather personal and financial information from the target.
- Pretexting: Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.
- Scareware: Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.
- Water-holing: A watering hole attack is when the attacker attempts to compromise a specific group of people by infecting websites they are known to visit and trust in order to gain network access.
- Diversion theft: In this type of attack, the social engineers trick a delivery or courier company into going to the wrong pickup or drop-off location, thus intercepting the transaction.
- Quid pro quo: A quid pro quo attack is one in which the social engineer pretends to provide something in exchange for the target's information or assistance. For instance, a hacker calls a selection of random numbers within an organisation and pretends to be calling back from tech support. Eventually, the hacker will find someone with a legitimate tech issue who they will then pretend to help. Through this, the hacker can have the target type in the commands to launch malware or can collect password information.
- Honey trap: An attack in which the social engineer pretends to be an attractive person to interact with a person online, fake an online relationship and gather sensitive information through that relationship.
- Tailgating: Tailgating, sometimes called piggybacking, is when a hacker walks into a secured building by following someone with an authorised access card. This attack presumes the person with legitimate access to the building is courteous enough to hold the door open for the person behind them, assuming they are allowed to be there.
- Rogue: Rogue security software is a type of malware that tricks targets into paying for the fake removal of malware." (Rouse, 2020)

THE EFFECT ON ORGANISATIONS:

Unfortunately, corporate enterprises are at risk to these various attacks. The magnitude of employees results in various targets for social engineers. Real world examples of these attacks include the following:

- The 2011 data breach of security company RSA. An attacker sent two different phishing emails over two days to small groups of RSA employees. The emails had the subject line "2011 Recruitment Plan" and contained an Excel document attachment. The spreadsheet contained malicious code that installed a backdoor through an Adobe Flash vulnerability. While it was never made clear exactly what information was stolen, if any, RSA's SecurID two-factor authentication (2FA) system was compromised, and the company spent approximately $66 million recovering from the attack (Rouse, 2020).

- In 2013, a phishing scam led to the massive data breach of Target. A phishing email was sent to an HVAC (heating, ventilation and air conditioning) subcontractor that was a business partner of Target's. The email contained the Citadel Trojan, which enabled attackers to penetrate Target's point-of-sale systems and steal the information for 40 million customers’ credit and debit cards. That same year, the U.S. Department of Labor was targeted by a watering hole attack, and its websites were infected with malware through a vulnerability in Internet Explorer that installed a remote access Trojan called Poison Ivy (Rouse, 2020).

- In 2015, hackers gained access to the personal AOL email account of John Brennan, then the director of the CIA. One of the hackers explained to media outlets how he used social engineering techniques to pose as a Verizon technician and request information about Brennan's account with the telecom giant. Once the hackers obtained Brennan's Verizon account details, they contacted AOL and used the information to correctly answer security questions for Brennan's email account (Rouse, 2020).

A BRAVE NEW WORLD
THE LIBELIUM SMART WORLD
IOT AND FINANCE
IOT AND SECURITY
SOCIAL ENGINEERING
IOT AND BIG DATA
THE EFFECT ON ORGANISATIONS
AN AUDIT APPROACH
DEFENCE MECHANISMS
CONCLUSION
REFERENCE LIST

A BRAVE NEW WORLD
THE LIBELIUM SMART WORLD
IOT AND FINANCE
IOT AND SECURITY
SOCIAL ENGINEERING
IOT AND BIG DATA
THE EFFECT ON ORGANISATIONS
AN AUDIT APPROACH
DEFENCE MECHANISMS
CONCLUSION
REFERENCE LIST

AN AUDIT APPROACH:

Owing to various emerging technologies, business is ever changing and the audit practice is therefore affected. The following subtopics can therefore be accounted for when contemplating business initiatives.

Security: “Seventy-two percent of global IT and cybersecurity professionals surveyed by ISACA say there is a medium or high likelihood that an organisation will be hacked through an IoT device.” “IT auditors should perform a vulnerability assessment of such devices and consider conducting penetration tests on those systems periodically. Results of these procedures should be used to strengthen the security of IoT systems” (Salman, 2015).

Resilience: “IoT systems may support a business process that is either critical or time-bound, such as the delivery of perishable goods. IT auditors should assess whether controls are in place to recover IoT systems in the event of a failure. Auditors should determine whether management understands the potential business impact of an IoT system outage and whether appropriate and adequate policies, procedures, and processes are in place to timeously recover affected business processes in the event of an outage or disaster” (Salman, 2015).

Health and safety: “An important area internal auditors should assess is whether such IoT systems have undergone sufficient testing using appropriate test cases before being deployed into production. Furthermore, controls should be in place to ensure adequate testing is performed before upgrades, patches, and changes are made to IoT systems where health and safety is a significant risk” (Salman, 2015).

Monitoring: “Internal auditors should assess whether adequate monitoring controls are in place and whether all such controls have been operating effectively over time. Furthermore, auditors should assess whether exceptions and failures that occur are logged appropriately and resolutions to incidents are timeously recorded” (Salman, 2015).

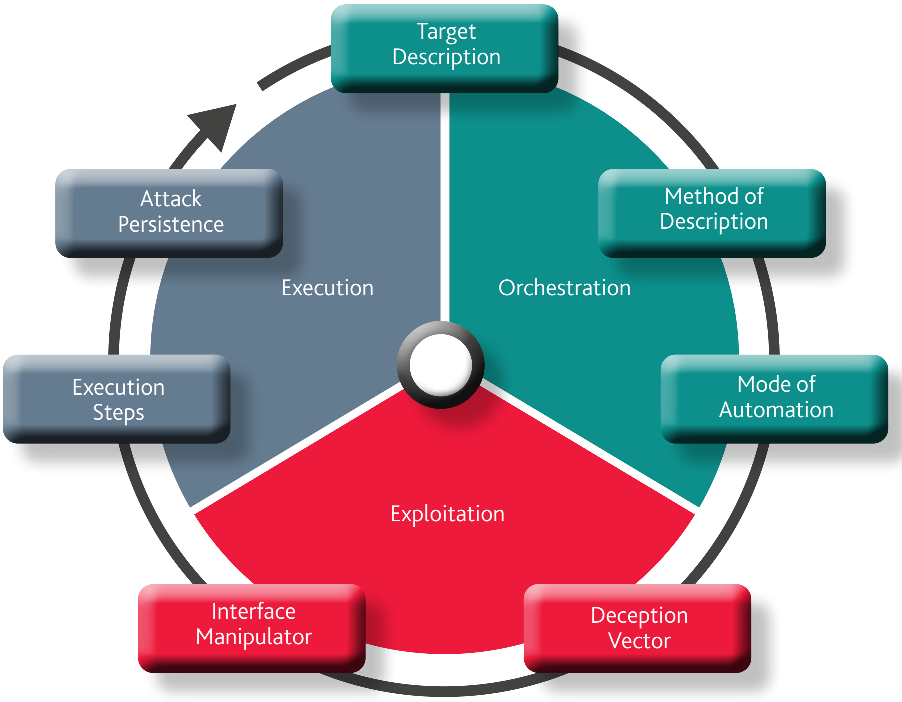
Scoping an IoT system: “Auditors should be vigilant to see where and when IoT systems are deployed by different departments at the organisation and prioritise IoT systems audits according to their critical and sensitive nature” (Salman, 2015).

IoT is being used innovatively to assist audit procedures. Drones are used to count stock and monitor crops while also monitoring building completion. IoT provides a variety of capable business-use cases, however sufficient security measures should be in place to ensure that the data is not corruptible.

DEFENCE MECHANISMS:

Thankfully, defence mechanisms against such threats do exist and are put into practice to try mitigate these threats. An effective mechanism is to break down deception vectors to build a range of defensive mechanisms. Through segregation, potential threats can be separated by their various similar traits and thereafter be categorised to provide precise solutions. Developers are thereby able to construct platforms to mitigate the segregated threats.

A high-level taxonomic classification criteria, supplied by (Hartfield and Gan, 2016) for social engineering attacks specifically with IoT.



The criteria focuses on orchestration, exploitation and execution.

Orchestration:

- Target description
  - How is a target chosen? Why is something/someone attacked?
  - Example: Geolocation is accessible.
- Method of distribution
  - How does the attack reach the target?
  - Is the system remote (On a network) or local (In need of monitoring and defending)?
- Mode of automation
  - Is the attack automated?
  - Automatically or manually executed? This helps determine behaviour and what the next step may be.

A BRAVE NEW WORLD
THE LIBELIUM SMART WORLD
IOT AND FINANCE
IOT AND SECURITY
SOCIAL ENGINEERING
IOT AND BIG DATA
THE EFFECT ON ORGANISATIONS
AN AUDIT APPROACH
DEFENCE MECHANISMS
CONCLUSION
REFERENCE LIST

Exploitation:

- Deception vector:
    - Do looks or behaviour deceive the user?
    - Within the IoT, it is not just GUIs that can be abused, but the physical appearance or state of a sensor node in a home/work/city automation system, as well (e.g., heating thermometer, heartbeat monitor, vehicle speed, traffic lights).
- Interface manipulator:
    - Depending on the system involved in an attack, it may be impractical or impossible to patch directly (e.g., pacemaker, legacy actuator). In order to reduce the scope of a defense, developers need to establish whether the deception vector in an attack occurs in code (e.g., embedded within the system or external) or abuses intended user space functionality built into the platform by design.

Execution:

- Execution steps:
    - Does the attack complete the deception in one step?
    - Model the effect that a single user action can have on the integrity of a platform, as it may be necessary to build in extra user authentication steps to commit actions.
    - An attack that relies on multiple user response steps may be detected earlier and more easily than a single-step attack, and before it completes, by looking for traces of its initial steps.
- Attack persistence:
    - Does the deception persist?
    - Persistent attempts can be modeled by a learning-based defense system to identify the deception's pattern of behavior in order to block it.
    - One-off deception attempts are by definition more dif¬ficult to detect and may be missed if a defense is only looking for patterns in system behavior or if the pattern is as yet unknown. This is known as Zero-day vulnerability.

To improve systems and software development, focused with a step by step approach, the secure software development life cycle (S-SDLC) can be made use of. It is important that IoT platform developers have a detailed understanding of how their system will interact with users, as well as how system functionality may affect the wider ecosystem in which the system may be deployed. Within the S-SDLC framework, in each lifecycle stage, the following key concepts can aid the development of IoT platforms and functionality that are resistant to deception-based attacks.

Requirements: Identify the attack surface for an IoT platform by clearly defining the intended functionality and its expected limitations.

Design: Pinpoint weak spots in the user interface that can be abused or vulnerabilities in data transfer and network communications that may allow attackers to inject malicious data or code or gather information about the user.

Coding: Employ static code analysis to determine whether the platform's programmatic features are deterministic to ensure that spoofed or injected data does not force the platform to exhibit a deceptive behavior toward the user.

Testing: Design and implement scenarios where different user behavior is arbitrarily executed.

Release/Maintain: Continuous monitoring and patching should be applied (Hartfield and Gan, 2016).

CONCLUSION:

The IoT has resulted in a variety of new innovative business procedures and opportunities, however, if not managed correctly, it can have detrimental consequences. This paper explored the uses of IoT as well as potential social engineering cyber-attacks and how to mitigate these issues. Through awareness, the S-SDLC and the implementation of procedures and policies, employees will be aware of these threats and mitigation will occur. New risks and opportunities present us with a variety of challenges. We must be aware of the fourth industrial revolution as it is here to change life as we know it.

A BRAVE NEW WORLD
THE LIBELIUM SMART WORLD
IOT AND FINANCE
IOT AND SECURITY
SOCIAL ENGINEERING
IOT AND BIG DATA
THE EFFECT ON ORGANISATIONS
AN AUDIT APPROACH
DEFENCE MECHANISMS
CONCLUSION
REFERENCE LIST

REFERENCE LIST:

BehrTech. 2020. 5 Industrial IoT (IIoT) Predictions For 2019 | Behrtech Blog. [online] Available at: <https://behrtech.com/blog/5-iiot-predictions-for-2019/> [Accessed 26 March 2020].

Careerfoundry.com. (2020). These Are The 17 Top Tech Buzzwords You Need To Know. [online] Available at: https://careerfoundry.com/en/blog/web-development/tech-buzzwords-to-learn/ [Accessed 11 Feb. 2020].

Dawex.com. 2020. Sell, Buy And Share Data. [online] Available at: <https://www.dawex.com/en/> [Accessed 26 March 2020].

Elon.edu. (2020). The 2016 Survey: The Future of IoT Connectivity – Imagining the Internet. [online] Available at: https://www.elon.edu/u/imagining/surveys/vii-2016/internet-of-things-infrastructure/ [Accessed 11 Feb. 2020].

Entrepreneur Council, Y., 2018. Council Post: 10 Big Security Concerns About IoT For Business (And How To Protect Yourself). [online] Forbes. Available at: <https://www.forbes.com/sites/theyec/2018/07/31/10-big-security-concerns-about-iot-for-business-and-how-to-protect-yourself/#64199a637416> [Accessed 26 March 2020].

Evans, D., 2011. [online] Cisco.com. Available at: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> [Accessed 17 March 2020].

Greenberg, A., 2015. Hackers Remotely Kill A Jeep On The Highway—With Me In It. [online] WIRED. Available at: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> [Accessed 26 March 2020].

Hajdarbegovic, N., 2020. Are We Creating An Insecure Internet Of Things (IoT)? Security Challenges And Concerns. [online] Toptal Engineering Blog. Available at: <https://www.toptal.com/it-developer/are-we-creating-an-insecure-internet-of-things> [Accessed 26 March 2020].

Hartfield, R. and Gan, D., 2016. Social Engineering In The Internet Of Everything | Cutter Consortium. [online] Cutter.com. Available at: <https://www.cutter.com/article/social-engineering-internet-everything-492251> [Accessed 26 March 2020].

Hoenes, C., 2019. Kill The Password Before It Kills You – IDEE Gmbh Blog. [online] IDEE GmbH. Available at: <https://getidee.com/kill-the-password-before-it-kills-you/> [Accessed 26 March 2020].

Houkom, T., 2018. What Is The Internet Of Things? IoT & Smart Home Tech. [online] Frontsteps.com. Available at: <https://www.frontsteps.com/blog/the-internet-of-things-iot-explained> [Accessed 3 April 2020].

How the Internet of Things will change finance. 2019. How The Internet Of Things Will Change Finance. [online] Available at: <https://theworldnews.net/sg-news/how-the-internet-of-things-will-change-finance> [Accessed 26 March 2020].

Libelium.com. 2020. Libelium Smart World Infographic – Sensors For Smart Cities, Internet Of Things And Beyond | Libelium. [online] Available at: <http://www.libelium.com/libelium-smart-world-infographic-smart-cities-internet-of-things/> [Accessed 26 March 2020].

Midrack, R., 2019. What Is So Smart About A Smart Fridge? [online] Lifewire. Available at: <https://www.lifewire.com/smart-refrigerator-4158327> [Accessed 17 March 2020].

Miles, C. and Miles, C., 2017. Blockchain Security: What Keeps Your Transaction Data Safe? - Blockchain Pulse: IBM Blockchain Blog. [online] Blockchain Pulse: IBM Blockchain Blog. Available at: <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/> [Accessed 26 March 2020].

Muddana, V., 2020. What Is The Future Of IoT Or Internet Of Things In Next 5 Years? [online] Softscript Solutions Blog. Available at: <https://www.softscripts.net/blog/2019/01/future-of-IoT/> [Accessed 17 March 2020].

Newman, D., 2020. Top 5 Digital Transformation Trends In Insurance. [online] Forbes. Available at: <https://www.forbes.com/sites/danielnewman/2017/09/05/top-5-digital-transformation-trends-in-insurance/#6eeabf2230ba> [Accessed 26 March 2020].

Ngak, C., 2013. Baby Monitor Hacked, Spies On Texas Child. [online] Cbsnews.com. Available at: <https://www.cbsnews.com/news/baby-monitor-hacked-spies-on-texas-child/> [Accessed 26 March 2020].

Rouse, M., 2020. What Is IoT Security (Internet Of Things Security)? - Definition From Whatis.Com. [online] IoT Agenda. Available at: <https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security> [Accessed 26 March 2020].

Rouse, M., 2020. What Is Social Engineering? - Definition From Whatis.Com. [online] SearchSecurity. Available at: <https://searchsecurity.techtarget.com/definition/social-engineering> [Accessed 26 March 2020].

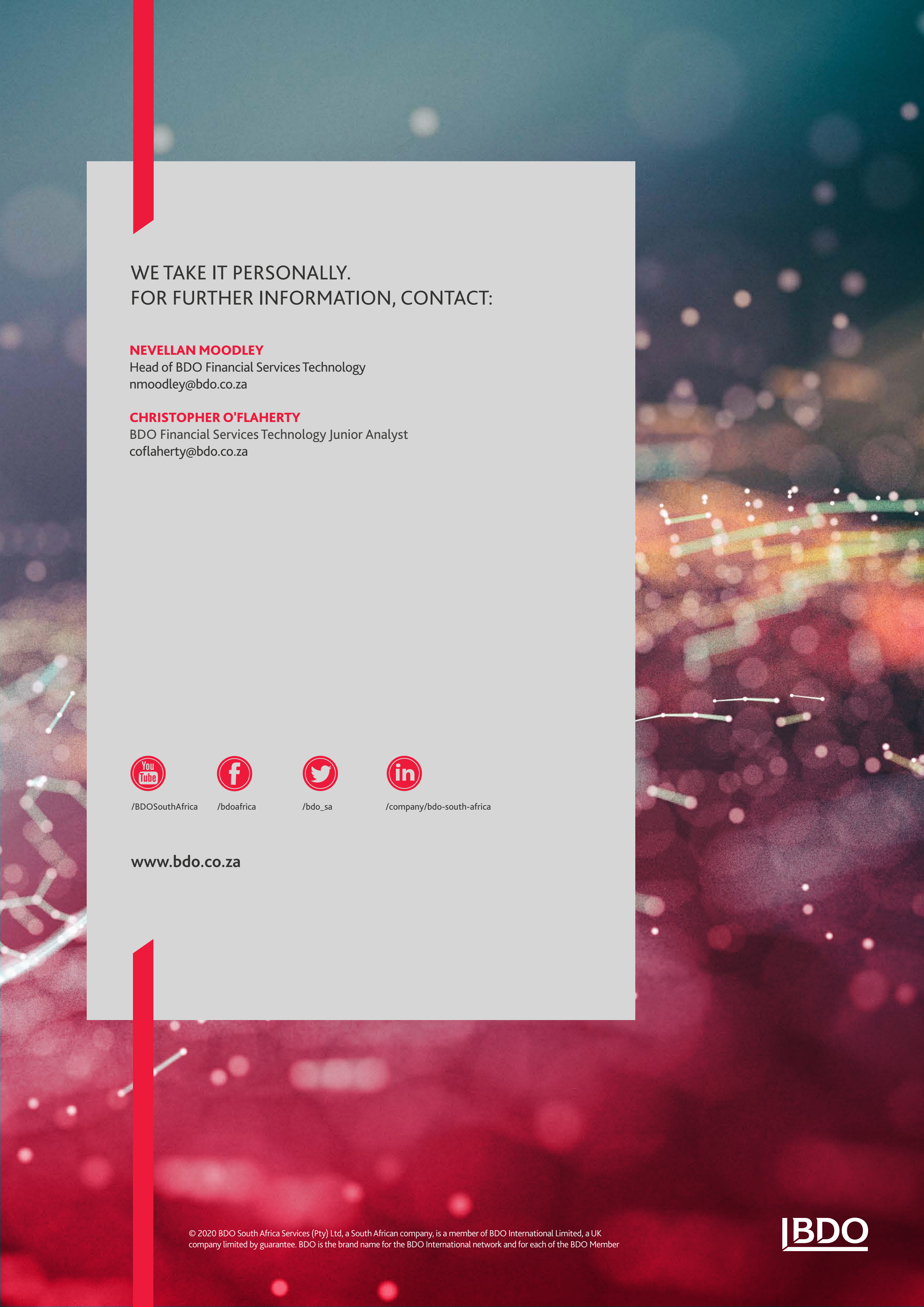
Salman, S., 2015. Auditing The Internet Of Things. [online] Iaonline.theiia.org. Available at: <https://iaonline.theiia.org/2015/auditing-the-internet-of-things> [Accessed 3 April 2020].

TechRepublic. (2020). Top 10 emerging technologies of 2019. [online] Available at: https://www.techrepublic.com/article/top-10-emerging-technologies-of-2019/ [Accessed 11 Feb. 2020].

Wakabayashi, D. and Satariano, A., 2019. Google To Buy Fitbit For $2.1 Billion. [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/11/01/technology/google-fitbit.html> [Accessed 26 March 2020].

World Economic Forum. (2020). The Fourth Industrial Revolution: what it means and how to respond. [online] Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ [Accessed 11 Feb. 2020].

A BRAVE NEW WORLD
THE LIBELIUM SMART WORLD
IOT AND FINANCE
IOT AND SECURITY
SOCIAL ENGINEERING
IOT AND BIG DATA
THE EFFECT ON ORGANISATIONS
AN AUDIT APPROACH
DEFENCE MECHANISMS
CONCLUSION
REFERENCE LIST



WE TAKE IT PERSONALLY.
FOR FURTHER INFORMATION, CONTACT:

NEVELLAN MOODLEY
Head of BDO Financial Services Technology
nmoodley@bdo.co.za

CHRISTOPHER O'FLAHERTY
BDO Financial Services Technology Junior Analyst
coflaherty@bdo.co.za

/BDOSouthAfrica /bdoafrica /bdo_sa /company/bdo-south-africa

www.bdo.co.za