Safe communication should be on still.

Have to target.
Enthralling reality is this.

PODBOT CS

When AI and IT interweaves - eventuates a new conception nascence.
Most essential device ever

Project description and profit outlook

How can we provide better security for IoT devices?

We assert that cybersecurity can be improved not solely with technology improvements, while this is the main aspect.

How important the technology improvement related to cybersecurity?

After a few statements, speculations, facts investigation, we could answer the questions above; while the right juristic basis, knowledge has owned, organised and ready to use.

> *As the developer of the new way technology and ADSC (Artificial Differentiated-Sophisticated Consciousness), I believe that full improvement of IoT devices should bring back the low (zero) risk data sharing, while, need to involve people to evolve the security processes.*

The Internet of Things is Going to Change Everything About Cybersecurity

All we know that the cyber threats are exploding globally and data breaches have led mainstream businesses to spend over $93 billion (worldwide) in past year (2017) on stopping cybercrime.
But all we know that this mission was unsuccessful.

Hackers globally have attacked social institutions, other important/non-important databases, etc.

Thence, the cyber-attacks against IoT devices are more frequent as before, because the hackers recognised the weak points in systems, of IoT devices. They got cheap big data and information sets.

The companies, institutions anticipate that a third of hacker attacks will be targeting shadow IT and IoT by 2020 and at all weak endpoints. Every non (weak) - secured connected/non-connected device, information, data remain as a potential victim in the closest future, until the moral or the attitude, behaviour does not change.

The time has arrived now, do something to strengthen your organisation security.

> *"Executives who are preparing to handle future cybersecurity challenges with the same mindset and tools, that they have been using all along are setting themselves up for continued failure."*

No doubt, old methods, solutions of defending enterprises from cyber-attacks are time to time unsuccessful, nevertheless, new security solutions are certainly needed to defend the sensitive data and all IoT devices.

> *"Hackers could reach the endpoint hardware/software tool by careless, untrained users' negligence or an unmanageable, defective hardware key, wrong settings or inadequate secure policy/protocol."*

You Should Avoid the Attacks

Never will enough to use some firewall, antivirus, malware removal tool, necessarily enlist new generation hardware and intelligent software methodologies.

Do not take people out of the security equation and do not buy more unnecessary looking existing IT protection gadgets to enhance the confusion.
Just trust and use a new methodology/device for IoT devices protection.

> *"It can't be denied, however, that in the age of increased social-engineering attacks and unmanaged device usage, reliance on a human-based strategy is questionable at best…*
>
> *A virus or an infected code is susceptible to airborne attacks, although hacker certainly not require standing close to the attacked device, enough a user may have productivity goals in mind do as usual, but there is simply no way you can rely on employees to use them within acceptable security guidelines. Users forget the proper settings, a system damage occur, etc."*

It is time to relieve your staff (partners, customers, etc.) of the cybersecurity burden.

You must do better-equipping users, relieving them from the cybersecurity burden, while the conventional and effective business wisdom remains true that the appropriate solutions must involve people, process and technology answers, IMPORTANT surplus instruction:

by the best intelligent protocol, coordination what should be provided by a complex security system.

> *"The appropriate solutions must involve people, process and technology answers, by the best intelligent protocol-, and coordination."*
>
> *"I want to say that I certainly agree that we need much better security built into IoT devices. I certainly think IoT security is at the cutting edge of cyber-issues."*
>
> *By Dan Lohrmann / 30 of December 2017*

Take a look at a new dimensional approach security protocol system (ADSC) and the device

- How use staff our IoT devices, the system without high risk?
- How set up our IoT device for the best security level with or without staff involve?
- What protocol or policy could build, which is the clearest, evident for all?
- How use protocol/policy system?

Almost everyone - except criminal hackers - would like to have IoT devices shipped most secure by default or secure by design with a hack-proof seal of approval on every IoT device.

WE DO NOT PROMISE ANYTHING. WE DO IT. WITHOUT COMPROMISES.

No doubts that much more need to be done with the security built into all technology, and it would be great if we could dramatically reduce IoT security flaws and the potential number of mistakes that can be made by end users.
The intelligent user authentication is the first step to improve the security of IoT devices, while the second is the safety policy/protocol system evolving by a built-in, intelligent consciousness provision.

However, bring to the fore effective security consciousness training (because not enough to experience the security, need to eternally feel that) and/or a comprehensive security culture - that I call policy/protocol - against better technology is a serious mistake and ultimately leads down on a path to dismal failure, therefore the importance to entail both.
Security awareness training without technology evolution is a conventional "mule", while

the security artificial consciousness (intelligence) improvement with technology revolution is the future.

You should certainly agree with that goal to build more-secure IoT devices and to install intelligent software, protocol system.

WE SHOULD AIM TO AUTOMATE AS MUCH SECURITY AS POSSIBLE - should we strive to build secure, smart devices with safest protocol system.

Of course. And ... the PODBOT CS with ADSC that has removed the potential for most end-user errors or security mistakes from the organisation system.
Nevertheless, training and working with people and processes to protect data will never be an optional extra for secure enterprises, this should be the default, it confirms the raison d'être of ADSC (Artificial Differentiated-Sophisticated Consciousness).

The holistic approach is required for IoT security.
If the organisations' leaders need to pick technology protections over enabling people with better awareness training and engaging in cyber-exercises, choose the AI-based technology (ADSC).

Better cybersecurity protections for IoT requires improvements in

- people,
- process,
- technology.

ADSC and PODBOT CS create a cyber policy/protocol following these rules

User log in policy

- Identify,
- Authenticate,
- Allocate permissions,
- Let users use IoT as usual.

Identify by motion

- Authenticate by face (countenance) and voice; if all these have not got a proper result, by password
- Allocate permissions by ADSC.

Security protocol

- Create a closed OS. Do not let crosslink of operations/functions,
- Let system creates log about every event,

- Do not let internet connection, if not necessary,
- Create a "faraday cage" for the IoT device,
- Isolate users (by isolation, managers could more effective way locate, identify the problem(s). You could know problem quality, location, nature)

All we are thought is smaller or larger group, team, not globally.

Just do it with AI.

Going forward.

The PODBOT CS with ADSC have a duty to achieve and increase the Security against 3rd Parties and Hackers; while able to increase the Efficiency of Companies' Communication, Data storage and real-time Synchronisation between connected IoT Devices.

The several past few Years we have worked hard to elaborate a Computer Server - Central Super Communication-computer Server - what has wide range Possibilities:

- to save Users' Identity,
- keep confidential and sensitive Data in Safe,
- cares (protects) connected/accommodated IoT (Portable Devices, computers, other equipment).

Our main goal was that to invent, develop Something significant, unique, clever IoT Device for physical protection of Portable Devices, connected gadgets.

What is important?

The real-time data/information synchronisation

and

The real-time high-level data/information protection.

This Conception has been released.

The Device able to accommodate Portable Devices; treats wirelessly connected Devices, Tools, Equipment too. It is important because the Future is the Mobile Communication Solver Devices, at Portable Devices (Tablets, Smartphones) - the tendencies prove that.

The heavy Companies use these Devices and would to know everything about its Partners, Co-workers, Colleagues, and everything about finished Works.

Want to get real-time Information about Data flows, Events and would to communicate on the highest safety Level ever.

To consider the above-mentioned Solutions, I decided that I develop this Device, and thus I would share this Tool and Solution with the Australian Government.
Related to the Aim to save the Country against phishing and Hacker attacks.

I am an Innovator, Developer, who see the Potential in Solutions, which could to make the World Safest Place.

This is a great Device, which has wide range Opportunity in Cyber-Defence Subject.

Exactly, what is PODBOT CS?

1. Powerful Central Super Communication-computer Server.

2. IoT (Portable Device and other equipment) device deploy/protector (managing) complex Hardware.

3. ADSC (Artificial Differentiated Sophisticated Consciousness) Tool - more than a virtual assistant, it is a real security manager with awareness.

4. Data/Information protector, partner in everyday life.

PODBOT (CS) Communication Server manufacturing – Project

Financial Details of PODBOT CS Project

In the following, you will find details about PODBOT CS Project profitability. If you want to reach the speculations spreadsheet, just open it from this document.

Financial specifics

1. Investment claim: Have to adjust the limit due to between at least AU$ 2.9 million or at least AU$ 12.8 million in scheduled phases. The phases and the investment amount are depending on the prototype(s) and software production. (The minimum smaller amount is for some specific software, while the minimal bigger investment contains at least 2 pc prototypes. During the project, have to intend to develop 9 different type of device with different material use and different functions, capacities for market demands. The different types of devices could widen the market coverage.)
2. This project has joint finance opportunity with the Defence Ministry of Australian Government with 10 to 50 percent non-refundable intensity and with 30 percentage propitious credit. If the project has the proper investment amount, then it could be starting.
3. The project is able to provide 5 to 10 percent profit rate for the investor(s), it is depending on the expected duration of the investment. The project uses 5 years calculation after the first 3 years developing time period finish.
4. The project's success (return) index: 161% (the principal repaid and got 61% profit), expected net profit is: AU$ 32 million at the end of #5 year.
5. Project schedule: 4-step development, consistent tasks execution and flexible financing opportunities - it is depending on the prototype manufacturing and software production (the following time periods are for the minimum AU$ 12.8 million investment):
    A. 1. phase: 6 months, AU$ 2.9 m
    B. 2. phase: 18 months, AU$ 7.5 m
    C. 3. phase: 6 months, AU$ 1.3 m
    D. 4. phase: 6 months, AU$ 1.1 m

Sales specifics

1. The development time interval: expected 3 years, after the first phase the pre-sales could be starting - if the investment is the minimum AU$ 12.8m. If the investment is smaller, then the development time interval minimum one and a half year, in this case, the sales schedule is changing.
2. The project has software and hardware branch, these elements could increase the sales and decrease the risk,
3. Target market:
    - A. Governments and defence ministries,
    - B. Educational institutions,
    - C. Medium and heavy corporations:
    - D. Production,
    - E. Service,
        - a. Logistics,
        - b. Robotics,
        - c. Education,
        - d. Telecommunication.
        - e. Agriculture.

4. Of course, the final product(s) has high relevance level in the international market (saleable). PODBOT CS is the perfect choice for medium-, and large sized corporations which have a lot of portable devices in use, and there are important the safety criteria of communication, data/information synchronisation, while would REAL-TIME tracking and SYNCING the devices, tools, staff. The transparency, controllability and SECURITY effort of these elements have must have importance.

Stability enhancer specifics

1. Security demands of corporations, governments and institutions ensure the success and reliability (profitability) of this project, however, the device has a lot of ability on the fields of cyber defence, software/hardware security. These abilities reflect the current and latent market demands and have to give a birth to a device what is profitable for developers and the investor(s) consortium.
2. The main strengths of PODBOT CS are the powerful hardware configuration, the software availability and the security protocol system, and the Artificial Intelligence security system (ADSC). This calibration ensures the attractiveness, while the device redeems the exist computer parks or increases their efficiency at the corporations (therefore could create different type devices that could have to widespread use at different sized companies).
3. We could rely and forming cooperation (alliance) with portable device manufacturer brands (Apple, Samsung), because these companies would gain more market share at company sector (our device offers support for portable devices that are manufactured by the mentioned brands. Our device support for portable devices is a key to gain more market share). The partnership with great brands could increase the reliability of our project.
4. The device has no explicit competitors, this is precedent new development on the market. There were several attempts to build a mass supporter (deploy) device for portable devices (for example USA, Apple - Bretford). These attempts have great results, but they could not have become popular because their functionalities were sidedness. Our device (Communication Server) should exploit and expand beyond functionality benefits, while demonstrates the future technology the AI security system development.

This project means a small amount of the anticipated spending of cyber-security, but its significance and benefits could achieve remarkable market successes.
By our preliminary correspondence with Defence Ministry of Australia (Mr Hon. Dan Tehan), I can state that this project has significant attention by Cyber Defence department. The broad spectrum of the project's security palette led to the trust of the Australian government, which would provide a worthy place in the Australian Cyber defence program if the project has a 50-90% own resource.

Thank you for your attention - If you would like to easily understand the profitability of the project, please download the PODBOT CS Cash Flow spreadsheets which created by experts' verification and approval, click here to download.

John Buresch
https://uk.linkedin.com/in/jaburesch
more information: https://www.podbot.uk

Email:	jburesch@me.com
Phone:	(+44)07894263737