How will the Internet of Things (IoT) revolutionize contract management for Projects and Programs Management?[1, 2]

Thibault Kibler

INTRODUCTION

The Internet of Things (IoT) is the extension of the Internet to things and places in the physical world. While the Internet does not usually extend beyond the electronic world, the IoT represents the exchange of information and data from real-world devices over the Internet. It takes on a character universal for objects connected to various uses, in the field of e-health, home automation, retailed and so forth. Every company starts looking into it; it is an incredible golden goose. Starting from Google to Apple, start-ups or SME, everyone is now running for IoT.

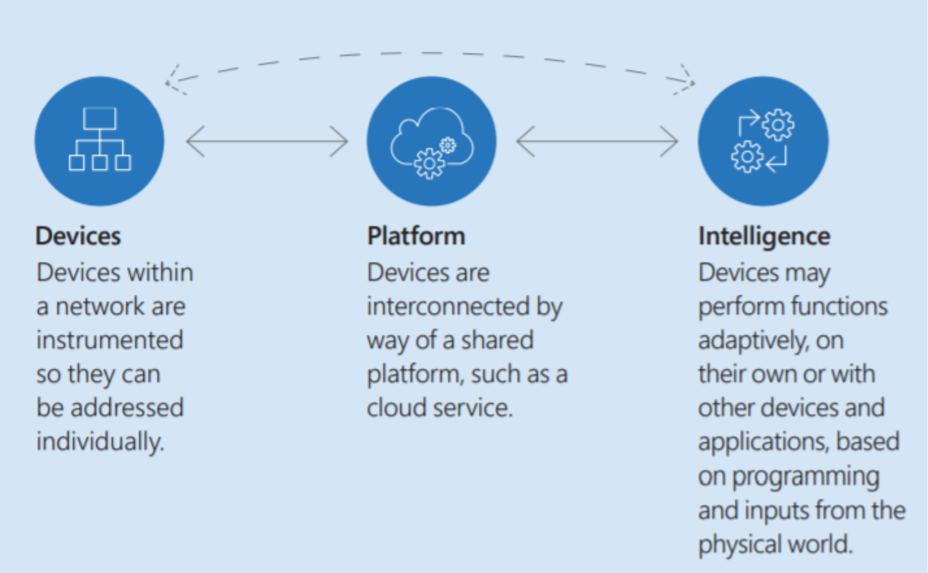

Devices
Devices within a network are instrumented so they can be addressed individually.
Platform
Devices are interconnected by way of a shared platform, such as a cloud service.
Intelligence
Devices may perform functions adaptively, on their own or with other devices and applications, based on programming and inputs from the physical world.

Figure 1: What is IoT?[3]

[1] Editor's note: This paper was prepared for the course "International Contract Management" facilitated by Dr Paul D. Giammalvo of PT Mitratata Citragraha, Jakarta, Indonesia as an Adjunct Professor under contract to SKEMA Business School for the program Master of Science in Project and Programme Management and Business Development. http://www.skema.edu/programmes/masters-of-science. For more information on this global program (Lille and Paris in France; Belo Horizonte in Brazil), contact Dr Paul Gardiner, Global Programme Director, at paul.gardiner@skema.edu.

[2] How to cite this paper: Kibler, T.G.A. (2019). How will the Internet of Things (IoT) revolutionize contract management for Projects and Programs Management? *PM World Journal*, Vol. VIII, Issue I (January).

[3] Abendroth, B., Kleiner, A., & Nicholas, P. (2017). Cybersecurity policy for the internet of things. Microsoft.

Previsions said that by 2025, there would be 75.4 billion connected devices, equivalent to 10 IoT devices for every person on earth. It looks great. It can also be applied in companies, for example in the supply chain. It shows that it can increase the performance by 36%! This medium is undoubtedly incredible, and the booming is understandable. With more and more IoT devise, some questions start to rise such as data security, cyber attack, hacking, and so on. Now imagine that just by clicking on an object you sign a contract, how is this referred to? Can IoT devices function as agents? Meaning, are they legally allowed to create contracts on a user's behalf? So many questions and danger, and no real answer.

Following the definition of the Max Wideman's Comparative Glossary (MWCG), "In project management, that part of an organization responsible for managing a project from inception to closure as evidenced by successful delivery and transfer of the project's product into the care, custody and control of the Client or Customer"[4]. It is now clear that during the process of project management, time should be allocated to contract management! Because there is no real law yet on IoT, the contract management team aims to find a solution to frame it, every danger for the contractor must be analyzed to protect him, and on the overhand, contractees are not aware of the danger or internet. At a larger scale, we can look into program management, here the definition from MWCG: Program management is "the effective management of […]a collection of projects that together achieve a beneficial change for an organization" [5]. Everyone is running to get some cash from the golden goose. Moreover, these are not just simple projects; it is a real program and a change for companies to move into IoT. It is confined not only in one area; every sector is looking for IoT: construction, retail, bank, health, industry, and so forth. You need to be the best to not be flooded by concurrence.

Ten years ago IoT was a blue ocean but nowadays, this is a bit dangerous and scary red ocean[6]. Good and healthy program management is a must have, especially to take care of the data security, the more project you have, the bigger the risks. Many issues are raising such as: How should the courts assess the consent of the consumer when contracts are made using IOT devices? How manage all the data generated through thousands and thousands of IoT devices? Consent to mass consumption contracts was, of course, a problem even before the IOT. This has become a bigger problem with wrap contracts - where clicking, dragging and tapping were considered sufficient to sign an online contract. The IoT is threatening to make contractual agreement online even more fantastic with the introduction of e-agents. Each device can be a contract, and the consumer does not know it. "The more removed the consumer is from the act of contracting and the harder it is to access the actual terms, the less real the consequences of

[4] Wideman Comparative Glossary of Project Management Terms v5.5. (n.d.). Retrieved from http://www.maxwideman.com/pmglossary/PMG_P16.htm#Project%20Manager

[5] Wideman Comparative Glossary of Project Management Terms v5.5. (n.d.). Retrieved from http://www.maxwideman.com/pmglossary/PMG_P11.htm#Program%20Management

[6] More information about this marketing strategy: Kim, W. C., & Mauborgne, R. (2016). Blue ocean strategy: How to create uncontested market space and make the competition irrelevant.

that contract seem"[7]. How will you react if by just clicking on an app you are accepting that a company can use the tape of your connected camera? IoT is starting to get out of control: at the most basic level, many IoT devices have not incorporated computer security or hacking risks into their design. This leaves many weak points and flaws through which hackers and other cybercriminals can infiltrate information systems. Over the past two years, AT & T's[8] (American company) security operations center has experienced a 458% increase in IoT device vulnerability assessments.

Also, many IoT devices are not monitored properly. Nearly half of AT & T respondents admit that they are satisfied with estimating the number of connected devices they have; only 38% use management systems or software to identify connected devices and only 14% have a formal verification process. The contractor needs to define whether or not the customers are in charge, and if there is a leak, how the problem can be solved. Here below the leading causes of data breaches, leading to possible contract failure.

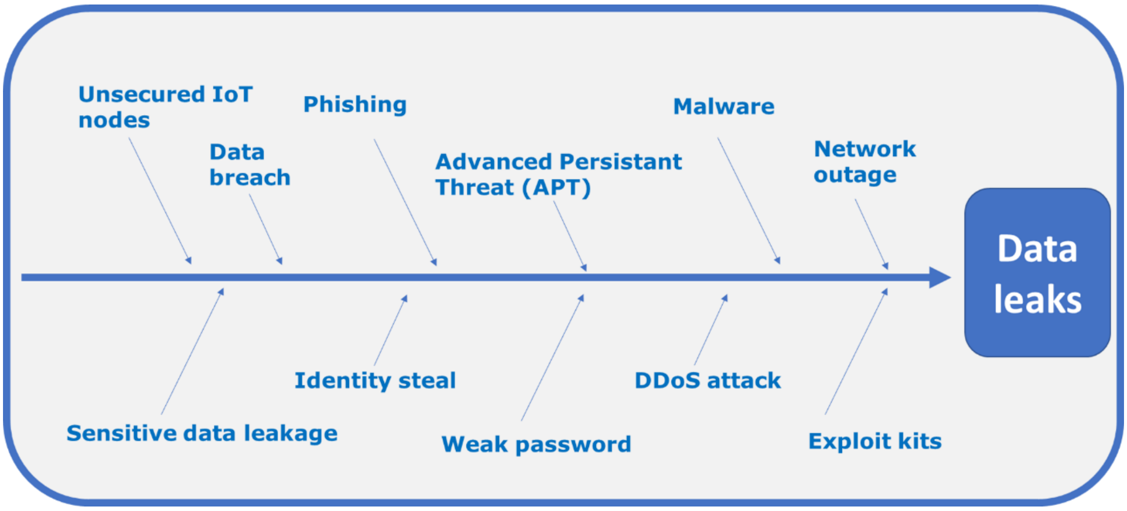


Figure 2: Root cause analysis[9]

IoT reflates the Big Data Race: by launching millions of devices, we are opening a real highway for hackers, the consumers are "signing" contract without even knowing it. This leads us to our real question, how will the Internet of Things revolutionize contract management for Projects and Programs Management? Some points can be easily prevented by doing training or informational campaign (weak password, exploit kits, malware, phishing). Other can't work because of the scale of the attack (DDoS, APT, Network Outage, Identity steal). That is why we

[7] Is Contract Law Ready for the Internet of Things? - Contracts. (2016, December 5). Retrieved from https://contracts.jotwell.com/is-contract-law-ready-for-the-internet-of-things/
[8] AT&T® Official - Entertainment, TV, Wireless & Internet - 6.4. (n.d.). Retrieved from https://www.att.com/
[9] By Author

will focus on Unsecured IoT nodes (when two IoT devices "speak" together, it is called a node) and the point that can be prevented by training or inform people.

Keywords: Internet of Things – Connected devices - Big Data – User knowledge – Contract management – Data Hacking

METHODOLOGY

Step 1: Summarize

As introduced, there is a big problem around data hacking and loss of information. We need to find the best methods to:

- Frame data hacking
- Secure data hacking.

Step 2: Identification of alternative solutions

First, we need to explain further the security. Most of IoT devices currently relies on machine-to-machine (M2M) technologies. In other words, IoT sensors talk to each other instead of talking to a centralized server. If your smart thermostat tells your dishwasher when to start, that communication goes over your Wi-Fi or Bluetooth network, even without going over the internet, you are taking significant risks. The Wi-Fi and Bluetooth protocols are easily hackable, but how do the two communication nodes know that the information coming from the other is allowed? Keep this word in mind, nodes. This is the most significant point of our research and the biggest issue. Each node is a possible door. Any M2M interaction requires a certain level of trust; only we have no way of predicting, or revoking it if an incident occurs. How can your dishwasher know someone has hacked your thermostat? By securing the nodes, we create a win-win situation: both the contractor and the contractee are safe.

Alternative Solution

As we need to find two solutions, we will make two lists of alternatives solutions. One solution will be about how to secure the nodes to make the contract safer for the contractor side. The other will be about framing the contract and train the end-user to make him aware of the danger of IoT.

Security of IoT nodes:

- *User-Managed Access (UMA):*

UMA[10] is an OAuth[11]- Based protocol designed to answer public concerns about privacy and individual consent. It is an open initiative and free to use. OAuth is an authorization framework framing third-party application to obtain limited access to an HTTP service. The goal of UMA is to create different user case, authorizations and prevent exterior people from entering the system.

- *TinyPK protocol:*

The purpose of the TinyPK [12]The protocol is to satisfy the authentication criterion via a key exchange between an external entity and a sensor network. In order to address resource issues and make the protocol viable, there are only public vital operations (data encryption and signature verification) that performed on the sensor. You can compare this to a tunnel between the external device and the IoT device. You ask for a connection with a public key (the name of the device) and a password paired with a timestamp (to prevent multiple tries,of connection in a short lap, it is the fundamental way to crack a password).

- *External specialized IAM (identity and Access management) contractor:*

The IAM contractor [13]will take in charge everything about data and network security. There are many companies specialized in it; I will not do the advertisement for each. That is why we will use a fictional company called ScIoT and will take as a hypothesis that the company is healthy and viable. The good point of this company is that it can do everything we need, but it has a cost.

- *Use of IoT monitors[14]:*

There a various IoT dedicated secured protocol [15]Such as Z-wave, Enocean, Zigbee, and so forth. Don't forget that Wi-fi or Bluetooth is also protocol, but they are not dedicated. By having a monitor "speaking" all these languages, you could put aside the nodes' problematic. Instead of having an app controlling each device, every IoT devices speak to one monitor, so there is only one big secured node. There will be still the problematic of the exchange with the global network, but the local one will be safer. The less app, software you use, the fewer nodes you have.

[10] La sécurité de l'IoT - Internet des Objets - JANUA. (n.d.). Retrieved from http://www.janua.fr/la-securite-de-liot-internet-des-objets/

[11] RFC 6749 - The OAuth 2.0 Authorization Framework. (n.d.). Retrieved from https://tools.ietf.org/html/rfc6749

[12] Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., & Kruus, P. (2004). TinyPK. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks - SASN '04. doi:10.1145/1029102.1029113

[13] What is identity and access management (IAM)? - Definition is from WhatIs.com. (n.d.). Retrieved from https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

[14] How the IoT is Changing Network Monitoring | Spiceworks. (2018, April 23). Retrieved from https://www.spiceworks.com/it-articles/iot-changing-network-monitoring/

[15] 11 protocols à connaître pour l'Internet des objects (IoT). (n.d.). Retrieved from https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about-fr

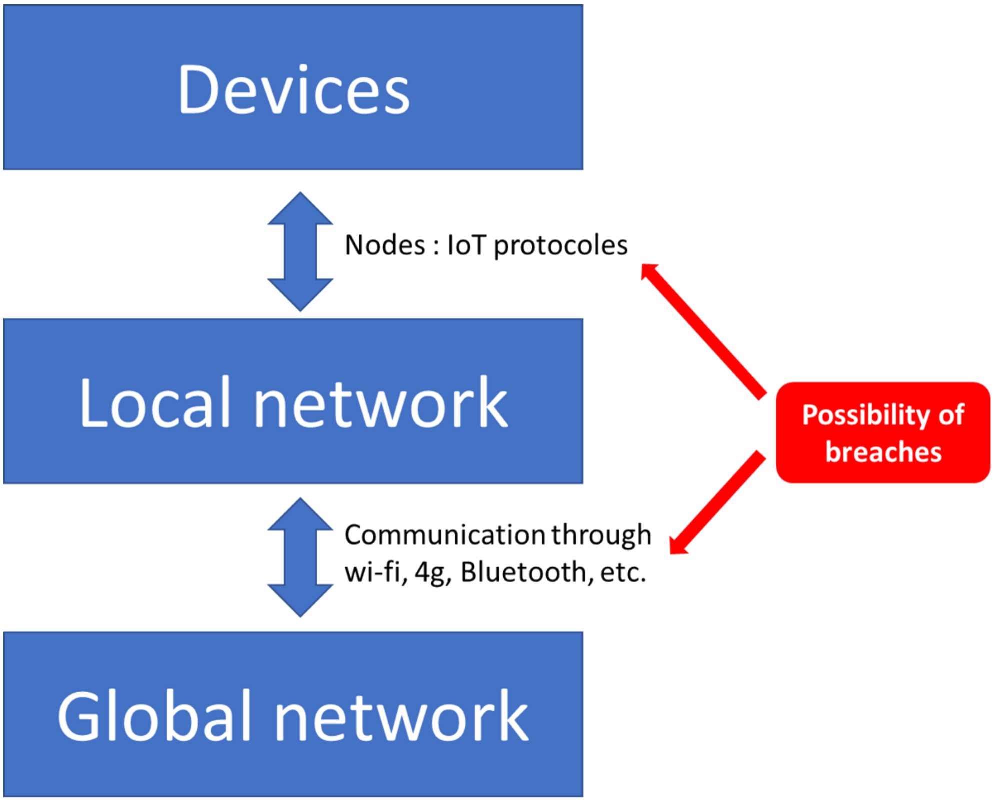


Figure 3: The different layouts of IoT[16]

By using a monitor, you can reduce the nodes inside your local network. It is like creating different cells, different private network. There will be fewer devices speaking together, for better security.

Framing data breaches and training users:

- *User knowledge, video version:*

Many breaches are just made by lack of knowledge of the user. Do you know that the top 3 passwords in 2017 are 123456, Password and 12345678. So even if you have the most secure system, a wrong user could open the door to a hacker. That is why you need to inform him by doing a presentation about a weak password, Exploit kits, Malware, phishing. As said earlier, by using IoT devices, the user is just signing a contract without knowing it. If you want to have a win-win situation, include in the contract that you are forming the user about the underlying data security, and then **create an informative video** [17]That will be launched for the first use of the product for example. If there is a data leak, and it is not a software defect (nodes, server attack, and so forth.), you will not proceed for the wrong use of your product. Any individuals

[16] By the author
[17] Designed by Contexture International | http://www.contextureintl.com. (2016, December 12). How to Teach With Videos. Retrieved from https://askatechteacher.com/2016/12/14/how-to-teach-with-videos/

can file direct claims for damages against both data controllers and data processors, so the supplier. That is why everything needs to be framed following YOUR COUNTRY standard[18]. Here are some European measures you need to look into (be aware that most of them are linked to data privacy):

- Privacy by design and default – to ensure that the default position is the least possible accessibility of personal data
- Consent
- Profiling – clearer guidelines on when data collected to build a person's profile can be used lawfully, for example, to analyze or predict a particular factor such as a person's preferences, reliability, location or health
- Privacy policies
- Enforcement and sanctions – violations of data privacy obligations could result in fines of up to 5% of annual worldwide turnover or €100m, whichever is greater

- *User knowledge, mail version:*

Same as before but instead of a video, we send him an explicative email, that he should read following the contract he signed. It should be design, concise, and first of all being informative! This is the main purpose. It should also be sent on a regular basis, such as a newsletter to keep the end-user informed[19].

- *User knowledge, workshop/event version:*

Same as the video version, but instead of a video, we do events and workshops [20]To make people aware of the security. For client customer, this can be done through a live hacking demonstration or workshop inside the company. For doing a great workshop/event, you need to prepare it (location, event, content) and think of how to make people involved (activities, mix up different types of people in each group, speech stick, and so forth.

- *User knowledge, basic contract version:*

In this version, we frame the possibility of data breaches in the contract, and we will not be involved if the user lost information because of the bad use of the product.

[18] IoTLAW. (n.d.). Retrieved from https://iotlaw.net/

[19] ten tips for creating great newsletters | Effective guide. (2017, September 28). Retrieved from https://www.mdirector.com/en/email-marketing-en/10-tips-for-creating-great-newsletters.html

[20] Planning a Workshop Organizing and Running a Successful Event. (n.d.). Retrieved from https://www.mindtools.com/pages/article/PlanningAWorkshop.htm

Attributes to measure, assess or evaluate each alternative

We need to analyze those alternatives. We will use a Multi-Attribute Decision Making (MADM). In my rating, I imagined the case of a specific company in order to order the top priorities. Here the case:

I am working in a big wealthy company working not a time to waste, security of my IoT environment is the top priority! The viability of the technology is also essential, the market changes a lot, and we do not want to lose time by jumping from a solution to another. Our image is also significant, we want to keep clients and attract others.

Here are the ranking criteria used for this method, for this ranking we used the five ways of measure project success: Schedule, Cost, Quality, Stakeholder satisfaction, and Performance to business case[21]:

Security of IoT nodes:

- Cost of implementation: cost is an essential problem in every company and should be considered.
- Time of implementation (Schedule): because IoT is a new technology moving fast, we need to be secured on our side as fast as possible.
- Viability[22] (Performance): a lot of IoT companies appears, create a protocol, and then die, making the protocol useless.
- Security of the nodes [23](Quality and Stakeholder): this is the purpose of this.
- A possibility of human error (Stakeholder): it is essential to consider that even the most secured nodes could be attacked because of bad user habits.

Framing data breaches and training users:

- Cost of implementation: cost is an essential problem in every company and should be considered.
- Time of implementation (Schedule): IoT is a new technology moving fast, we need to be secured on users' side as fast as possible.

[21] 5 Ways To Measure Project Success - ProjectManager.com. (2015, September 28). Retrieved from https://www.projectmanager.com/blog/5-ways-to-measure-project-success

[22] Top 10 criteria to choose the best IoT cloud platform. (n.d.). Retrieved from https://iotify.io/top-10-selection-criteria-for-your-iot-cloud-platform/

[23] Medium. (n.d.). Retrieved from https://hackernoon.com/how-to-choose-the-right-iot-platform-the-ultimate-checklist-

- Training of the user (Stakeholder, Quality, and Performance): this is the purpose of the solution and should be our top ordinal rank in our MADM. At the end of the formation/training, the user should
- Company image[24] (Stakeholder): As this will be in direct contact with the user, the image of the company is at stake.

Step 3: Development of Feasible Alternatives

We will now rank each attribute to perform this analyze, from the most important (1) to the least (5). It will help us to perform our MADM. You may wonder why this scale seems small and qualitative? It is normal IoT is a new technology, and these ranking will be purely personal. I made them following my researches. Don't hesitate to do your own; you have all the bibliography used at the end of this paper. Don't also hesitate to change the ordinal ranking following your case.

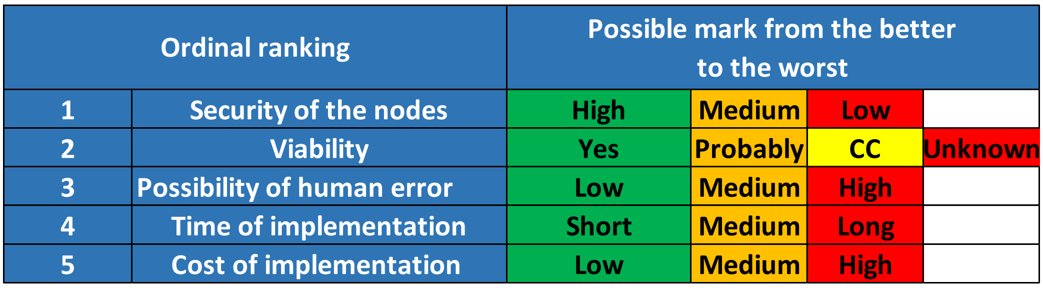
(1) We will give an ordinal ranking (1 is the best and five the worst) of each evaluating attribute brought up in the previous part, and choose the marking greed.

(2) Then we will mark each criterion following the marking greed.

<u>Security of IoT nodes:</u>

CC stands for continuous change.

(1) Ordinal ranking and marking greed



Ordinal ranking		Possible mark from the better to the worst			
1	Security of the nodes	High	Medium	Low	
2	Viability	Yes	Probably	CC	Unknown
3	Possibility of human error	Low	Medium	High	
4	Time of implementation	Short	Medium	Long	
5	Cost of implementation	Low	Medium	High	

Figure 4: Ordinal ranking and marking greed, security of the nodes[25]

(2) Marking

[24] Corporate Image - Encyclopedia - Business Terms. (0000). Retrieved from https://www.inc.com/encyclopedia/corporate-image.html

[25] By Author

Criteria\Solutions	UMA	TinyPK	ScIoT	Monitors
Security of the nodes	High	Medium	High	High
Viability	Probably	CC	Yes	Unknown
Possibility of human error	Low	Low	Low	Medium
Time of implementation	Medium	Medium	Medium	Short
Cost of implementation	Low	Low	High	Medium

Figure 5: Marking, security of the nodes[26]

We can see that UMA and ScIoT seem better.

Framing data breaches and training users:

(1) Ordinal ranking and marking greed

Ordinal ranking		Possible mark from the better to the worst		
1	Training of the user	Good	Quite good	Bad
2	Company Image	Excellent	Normal	Bad
3	Time of implementation	Short	Medium	Long
4	Cost of implementation	Low	Medium	High

Figure 6: Ordinal ranking and marking greed, framing and training[27]

(2) Marking

Criteria\Solutions	Video	Mail	Workshop	Basic contract
Training of the user	Quite good	Bad	Good	Bad
Company Image	Excellent	Normal	Excellent	Bad
Time of implementation	Medium	Short	Long	Short
Cost of implementation	Medium	Low	High	Low

Figure 7: Marking, framing, and training[28]

We cannot analyze without the weighting

Step 4: Sorting and weighting

We will now use the compensatory model to weight the result. Before doing this model, we can already reject two solutions, the monitors one (having an unknown about the technology is too risky, it means that if their company fail, all of our solutions will be useless) and the basic contract one (having a bad image is unacceptable).

[26] By Author
[27] By Author
[28] By Author

(1) We will first give a weight for each solution following this grid (particular case for viability, four different weights):

Color	🟥	🟧	🟩
Attribute weight	0	0,5	1

Figure 8: Weight grid[29]

The bigger the weight, the better for the company.

(2) Moreover, then weight these attributes to obtain the relative weighted result.

Security of IoT Nodes:

(1) Weight:

Criteria\Solutions	UMA	TinyPK	ScIoT
Security of the nodes	1	0,5	1
Viability	0,5	0,25	1
Possibility of human error	1	1	1
Time of implementation	0,5	0,5	0,5
Cost of implementation	1	1	0

Figure 9: Weight, security of the nodes[30]

It is tight. We need to use the relative weight to have a better view.

(2) Relative weight:

Attribute	Normalization				UMA (B)		TinyPK(C)		ScIoT (D)	
	Relative rank	Normalized weight (A)			(B)	(A)*(B)	(C)	(A)*(C)	(D)	(A)*(D)
Security of the nodes	1	5/15	=	0,33	1	0,33	0,5	0,17	1	0,33
Viability	2	4/15	=	0,27	0,5	0,13	0,25	0,07	1	0,27
Possibility of human error	3	3/15	=	0,20	1	0,20	1	0,20	1	0,20
Time of implementation	4	2/15	=	0,13	0,5	0,07	0,5	0,07	0,5	0,07
Cost of implementation	5	1/15	=	0,07	1	0,07	1	0,07	0	0,00
Total	15			1	SUM	0,80	SUM	0,57	SUM	0,87

Figure 10: relative weight, security of the nodes[31]

With these relative ranks, UMA and ScIoT seem to be the better solutions. We will analyze this in the next part: Findings.

[29] By Author
[30] By Author
[31] By Author

Framing data breaches and training users:

(1) Weight:

Criteria/Solutions	Video	Mail	Workshop
Training of the user	0,5	0	1
Company Image	1	0,5	1
Time of implementation	0,5	1	0
Cost of implementation	0,5	1	0

Figure 11: weight: framing and training[32]

(2) Relative Weight:

Figure 12: relative weight, framing and training[33]

Attribute	Normalization				Video (B)		Mail (C)		Workshop (D)	
	Relative rank	Normalized weight (A)			(B)	(A)*(B)	(C)	(A)*(C)	(D)	(A)*(D)
Training of the user	1	4/10	=	0,4	0,5	0,2	0	0	1	0,4
Company Image	2	3/10	=	0,3	1	0,3	0,5	0,15	1	0,3
Time of implementation	3	2/10	=	0,2	0,5	0,1	1	0,2	0	0
Cost of implementation	4	1/10	=	0,1	0,5	0,05	1	0,1	0	0
Total	10		SUM	1	SUM	0,65	SUM	0,45	SUM	0,7

With these relative ranks, the video and the workshop seem to be the better solutions. We will analyze this in the next part: Findings.

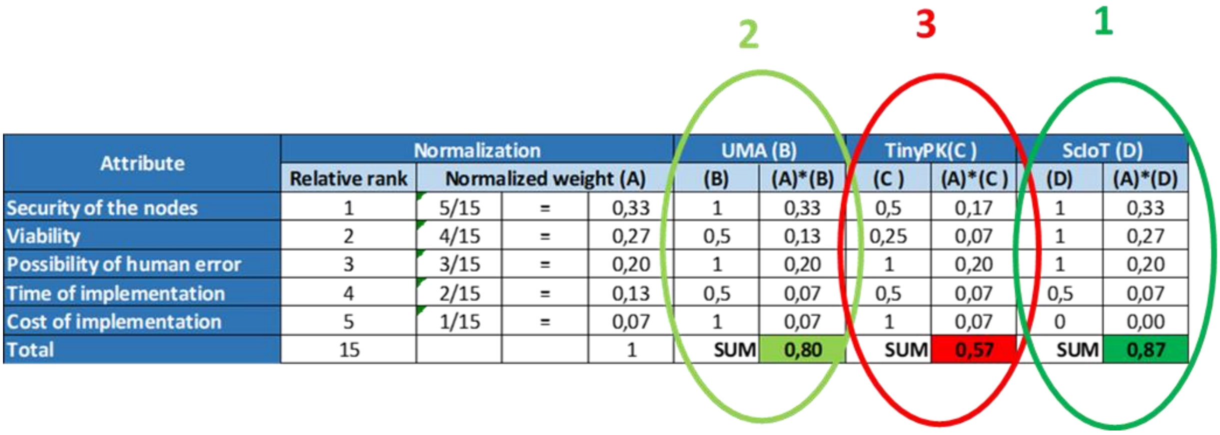
FINDINGS

STEP 5: Summarize

Here the rank order we get from the step 4 (from 1 the best to 3 the worst):

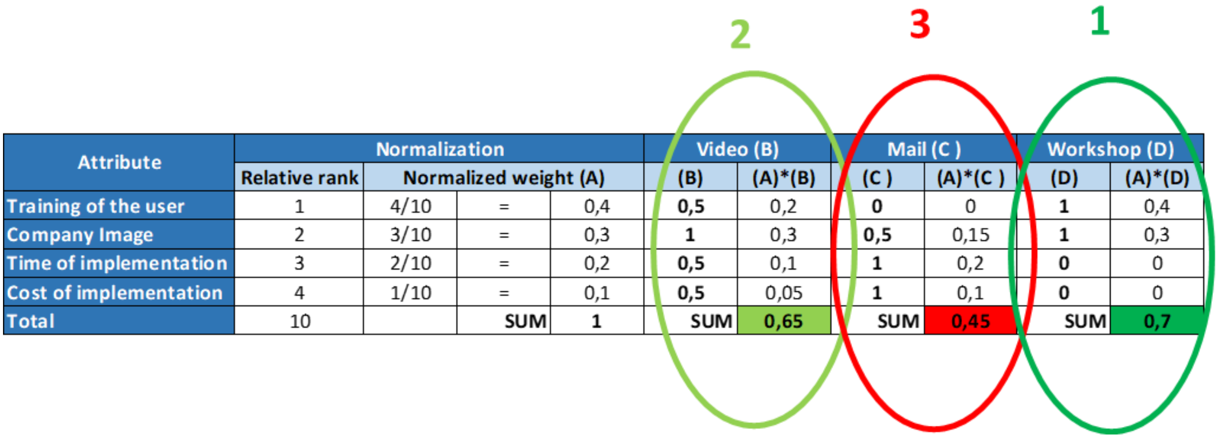
[32] By Author
[33] By Author

Security of IoT Nodes:



Attribute	Normalization				UMA (B)		TinyPK(C)		ScIoT (D)	
	Relative rank	Normalized weight (A)			(B)	(A)*(B)	(C)	(A)*(C)	(D)	(A)*(D)
Security of the nodes	1	5/15	=	0,33	1	0,33	0,5	0,17	1	0,33
Viability	2	4/15	=	0,27	0,5	0,13	0,25	0,07	1	0,27
Possibility of human error	3	3/15	=	0,20	1	0,20	1	0,20	1	0,20
Time of implementation	4	2/15	=	0,13	0,5	0,07	0,5	0,07	0,5	0,07
Cost of implementation	5	1/15	=	0,07	1	0,07	1	0,07	0	0,00
Total	15			1	SUM	0,80	SUM	0,57	SUM	0,87

Framing data breaches and training users:



Attribute	Normalization				Video (B)		Mail (C)		Workshop (D)	
	Relative rank	Normalized weight (A)			(B)	(A)*(B)	(C)	(A)*(C)	(D)	(A)*(D)
Training of the user	1	4/10	=	0,4	**0,5**	0,2	**0**	0	**1**	0,4
Company Image	2	3/10	=	0,3	**1**	0,3	**0,5**	0,15	**1**	0,3
Time of implementation	3	2/10	=	0,2	**0,5**	0,1	**1**	0,2	**0**	0
Cost of implementation	4	1/10	=	0,1	**0,5**	0,05	**1**	0,1	**0**	0
Total	10		SUM	1	SUM	0,65	SUM	0,45	SUM	0,7

Following these two ranking, we can exclude the email and the TinyPK that are too far behind following the weighting of the step 4.

Step 6: Selection of the preferred alternative

Security of IoT Nodes:

Following the step 5, UMA and ScIoT seem the best solutions. The TinyPK solutions are too behind.

If we now take a look about the attributes, the only difference between the two is the viability and the cost. As we consider we are a *big company* and cost is not a problem, the best solution is the ScIoT. These kinds of companies specialized in data security will be ready whenever there will be a change in security and maintain your system to keep it viable.

Here some example external specialized IAM contractor:

- Harmonie technologie[34]
- Globalsign[35]
- Nuxeo[36]
- NTT group[37]

Framing data breaches and training users:

Following the step 5, the video and the workshops are the best solutions. Based on the criteria, it is cheaper and faster to do a video but more useful for training with a workshop. Now we can think a bit about what do you want? If you are B to B, it will be better to do an excellent workshop to explain to the company you sold your product/services. If you are B to C, it will be easier to send a video.

The idealistic solutions would be to mix the two:

- An explanative video sent in any case
- A workshop for B to B[38] or a promotional and explanative event[39] for B to C (good for the image and the sell)

Step 7- Follow up

Now that we put forward the best solutions for our two cases (external specialized IAM contractor and doing a video/event), we can conduct a Pareto analysis to assess the double impact of these solutions on the security of our product (fewer data breaches, thus fewer disputes). "A Pareto Analysis enables the project control practitioner to identify the "significant few" from the "insignificant many" and use that information to prioritize which problems should be addressed."[40] The main problem of disputes[41]Is that it cost money! Following the Pareto law, about 80% of the effects are the product of 20% of the causes. Thus 80% of our problem is caused

[34] Conseil gestion des identités et accès IAM - Identity and Access Management. (n.d.). Retrieved from https://www.harmonie-technologie.com/iam-identity-access-management

[35] Certificats SSL et numériques GlobalSign. (n.d.). Retrieved from https://www.globalsign.fr/fr/

[36] ECM, DAM, Case Management par Nuxeo. (n.d.). Retrieved from https://www.nuxeo.com/fr/

[37] Nippon Telegraph and Telephone Corporation. (n.d.). NTT Home Page. Retrieved from http://www.ntt.co.jp/index_e.html

[38] Planning a WorkshopOrganizing and Running a Successful Event. (n.d.). Retrieved from https://www.mindtools.com/pages/article/PlanningAWorkshop.htm

[39] How to Plan a Promotional Event for Your Business - dummies. (n.d.). Retrieved from https://www.dummies.com/business/marketing/how-to-plan-a-promotional-event-for-your-business/

[40] GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from http://www.planningplanet.com/guild/gpccar/risk-opportunity-monitoring-and-control

[41] Nordby, H. (2018). Management and Conflict Resolution: Conceptual Tools for Securing Cooperation and Organizational Performance. Organizational Conflict. doi:10.5772/intechopen.72132

by data breaches and bad use of the product. By training and securing, we enhance the security on both sides and reduce disputes. We will use the fake business figure to illustrate the Pareto.

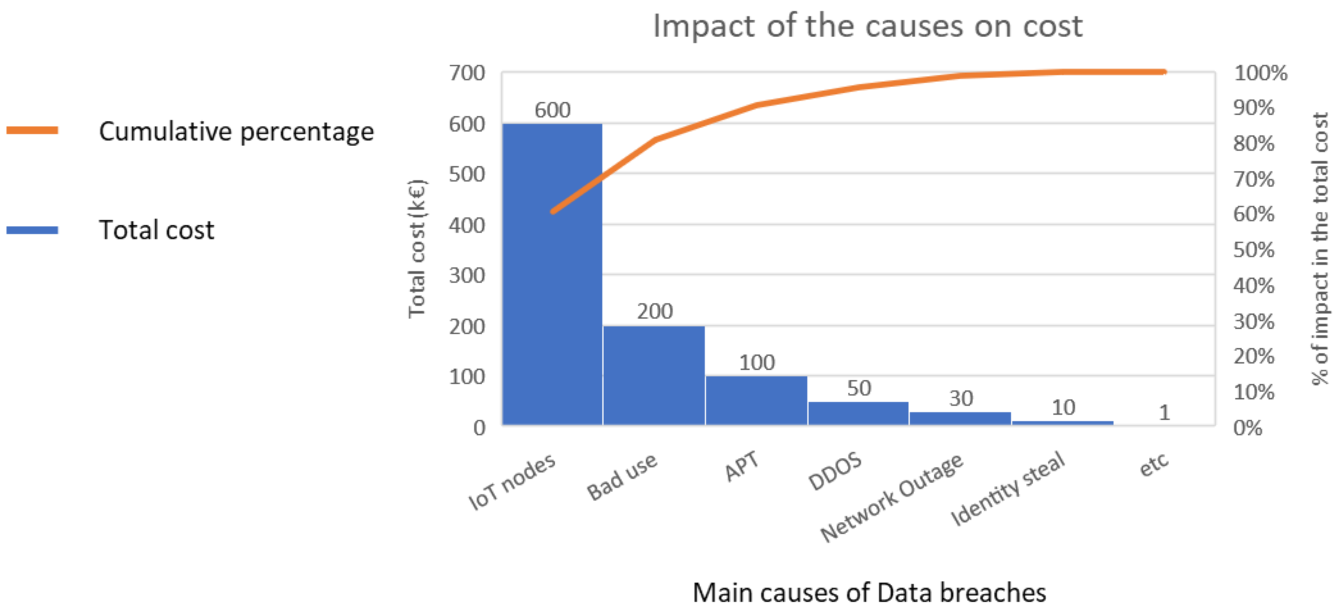


Figure 13: Pareto analysis, before implementation[42]

In this first analysis, we can see that without prevention disputes are going to profoundly impact the cost of the project, the public opinion but also the duration of the project.

Let's see now the impact of the causes of disputes on cost with better security on IoT nodes (probability of data breaches on nodes reduced by 99%), and better training. For the training, let's say they get 50% of what we explain to them[43], and we can touch at least 80% of our users. So, we got a reduction in impact by 40%. Here the new Pareto with these new numbers:

[42] By the author

[43] https://voir.ca/chroniques/prise-de-tete/2014/04/16/10-de-ce-quon-lit/

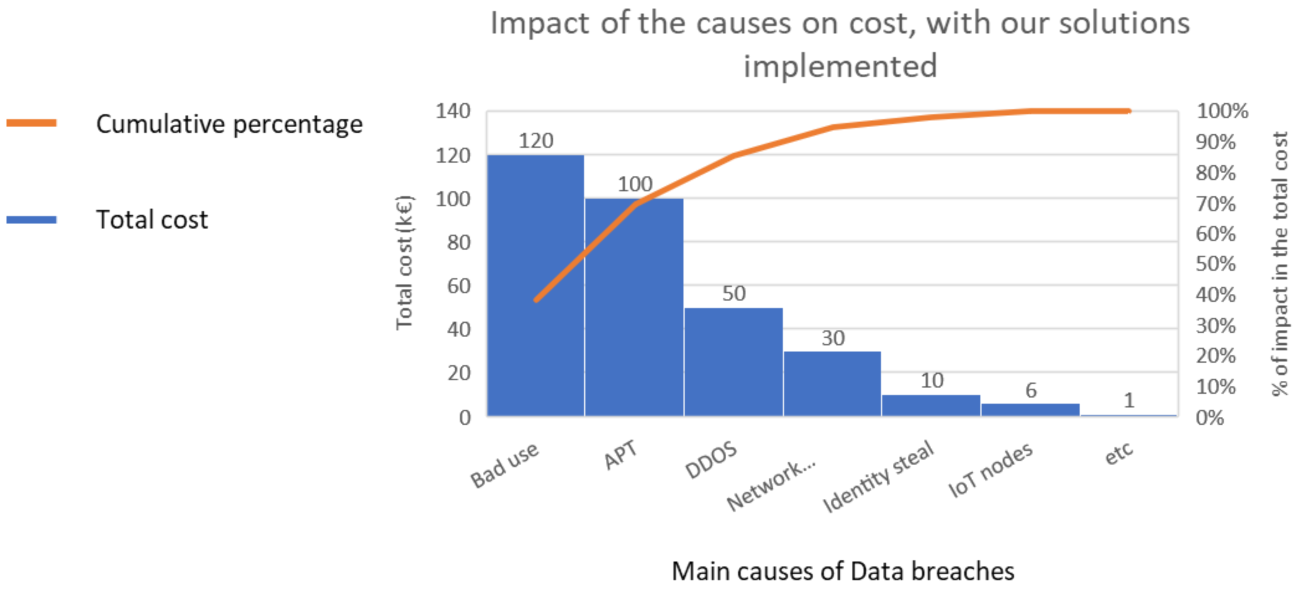


Figure 14: Pareto analysis, after implementation[44]

We can see an incredible reduction of the total cost in the case two, 317 k€ vs. 911k€ without our solutions. It is a reduction of the total cost linked to data breaches disputes by 69%.

CONCLUSIONS

The goal of this paper was to answer the following question: how will the Internet of Things revolutionize contract management for Projects and Programs Management?? We focused on unsecured IoT nodes and training and informing people, as they are the leading causes of data breaches which can then, guide us to contract failure/disputes.

Through this paper, we have assessed the alternatives on two sides: the security of the nodes and training of the user. We started with plenty of alternative solutions, and through an MADM process, we selected the best options on both scenarios: use an external specialized IAM contractor for the security and train the user by sending them an explicative video combined with a workshop or promotional event following if you are B to B/C. With the Pareto analysis, we proved that following the Pareto principle, by improving the two leading causes that are 80% of the effect on your project, you could reduce the cost impact by 70%!

This paper also raises questions: in our case, we cleared the security of the nodes, and the user are now the main causes of data breaches, followed by a DDOS attack on the server. How could we improve even more the end user training? Therefore, nothing will be linked to the nodes or bad use of the product. Thus, the only external event that we could not prevent will be framed

[44] By the author

in the contract, and assurances will take this in charge if there is any problem.[45] For example in France, civil responsibility [46]for the end user or a property damage and financial loss insurance for the contractor.[47]

BIBLIOGRAPHY

Intelligent supply chain | OpenText. (n.d.). Retrieved from https://www.opentext.com/campaigns/ai-iot/connected-supply chain?ldsrc=Paid%20Inbound&elqcampaignid=32134&utm_source=google&utm_medium=ppc &utm_campaign=bn-iot-connected-supply-chain-wp-text&gclid=EAIaIQobChMImanztdn43QIVBbftCh1_lQ6IEAAYAiAAEgKV1fD_BwE

B+B Smartwork. (2017). Iot gateways: what makes a gateway “fully functional”?

Contract Law in the Age of IoT. (2018, March 13). Retrieved from https://iotbusinessnews.com/2018/03/13/83045-contract-law-in-the-age-of-iot/

The World's First IoT Enabled Contract. (n.d.). Retrieved from http://www.legalalignment.com/blog/the-world-s-first-iot-enabled-contract

Is Contract Law Ready for the Internet of Things? - Contracts. (2016, December 5). Retrieved from https://contracts.jotwell.com/is-contract-law-ready-for-the-internet-of-things/

Blockchain : qu’est-ce qu’un Smart Contract et à quoi ça sert ? (n.d.). Retrieved from https://www.lemagit.fr/conseil/Blockchain-quest-ce-quun-Smart-Contract-et-a-quoi-ca-sert

Objets connectés et cyber-menaces : réveillons-nous! - Paris Innovation Review. (2018, September 18). Retrieved from http://parisinnovationreview.com/article/objets-connectes-et-cyber-menaces-reveillons-nous

Focus sur l'Internet of Things (IoT)... l'essentiel à savoir | Welcome to the Jungle. (2017, August 28). Retrieved from https://www.welcometothejungle.co/articles/focus-sur-l-internet-of-things-iot-l-essentiel-a-savoir

AT&T® Official - Entertainment, TV, Wireless & Internet - 6.4. (n.d.). Retrieved from https://www.att.com/

Wideman Comparative Glossary of Project Management Terms v5.5. (n.d.). Retrieved from http://www.maxwideman.com/pmglossary/PMG_P16.htm#Project%20Manager

[45] L'avenir des attaques distribuées par déni de service (DDoS). - Neotech. (2018, March 8). Retrieved from https://www.neotech-assurances.fr/lavenir-des-attaques-ddos/

[46] La responsabilité civile du particulier et son assurance. (n.d.). Retrieved from https://www.ffa-assurance.fr/content/la-responsabilite-civile-du-particulier-et-son-assurance?parent=74&lastChecked=120

[47] L'assurance des pertes d'exploitation de l'entreprise. (n.d.). Retrieved from https://www.ffa-assurance.fr/content/assurance-des-pertes-exploitation-de-entreprise?parent=79&lastChecked=150

GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from http://www.planningplanet.com/guild/gpccar/managing-change-the-owners-perspective

RFC 6749 - The OAuth 2.0 Authorization Framework. (n.d.). Retrieved from https://tools.ietf.org/html/rfc6749

La sécurité de l'IoT - Internet des Objets - JANUA. (n.d.). Retrieved from http://www.janua.fr/la-securite-de-liot-internet-des-objets/

Safe, S. (n.d.). SplashData - Powerful productivity tools. Retrieved from http://www.splashdata.com/

Q&A Identity & Internet of Things - DG - Identities of Things - Kantara Initiative. (n.d.). Retrieved from https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=67010606

La sécurité dans l'Internet des Objets. (n.d.). Retrieved from https://www.leblogduhacker.fr/la-securite-dans-internet-des-objets/

Abendroth, B., Kleiner, A., & Nicholas, P. (2017). Cybersecurity policy for the internet of things. Microsoft.

11 protocoles à connaître pour l'Internet des objets (IoT). (n.d.). Retrieved from https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about-fr

IoTLAW. (n.d.). Retrieved from https://iotlaw.net/

The Internet of Things. (n.d.). Retrieved from https://ec.europa.eu/digital-single-market/en/internet-of-things

How to survive upcoming IoT regulations and laws. (2017, August 21). Retrieved from https://www.iotworldtoday.com/2017/08/21/upcoming-iot-regulations-and-laws-how-survive-and-stay-compliant/

The legal considerations of the internet of things. (n.d.). Retrieved from https://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things

How to survive upcoming IoT regulations and laws. (2017, August 21). Retrieved from https://www.iotworldtoday.com/2017/08/21/upcoming-iot-regulations-and-laws-how-survive-and-stay-compliant/

Internet of Things (IoT) | DLA Piper Global Law Firm. (n.d.). Retrieved from https://www.dlapiper.com/en/africa/focus/internet-of-things/

Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., & Kruus, P. (2004). Tiny PK. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks - SASN '04. doi:10.1145/1029102.1029113

Kim, W. C., & Mauborgne, R. (2016). Blue ocean strategy: How to create uncontested market space and make the competition irrelevant.

What is identity and access management (IAM)? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

How the IoT is Changing Network Monitoring | Spiceworks. (2018, April 23). Retrieved from https://www.spiceworks.com/it-articles/iot-changing-network-monitoring/

Daum, K. (2013, September 6). How to Teach Anything to Anyone. Retrieved from https://www.inc.com/kevin-daum/how-to-teach-anything-to-anyone.html

Integrating the Internet: Risks and Solutions | Education World. (n.d.). Retrieved from https://www.educationworld.com/a_tech/columnists/poole/poole018.shtml

Designed by Contexture International | http://www.contextureintl.com. (2016, December 12). How to Teach With Videos. Retrieved from https://askatechteacher.com/2016/12/14/how-to-teach-with-videos/

Planning a Workshop: Organizing and Running a Successful Event. (n.d.). Retrieved from https://www.mindtools.com/pages/article/PlanningAWorkshop.htm

Medium. (n.d.). Retrieved from https://hackernoon.com/how-to-choose-the-right-iot-platform-the-ultimate-checklist-

Top 10 criteria to choose the best IoT cloud platform. (n.d.). Retrieved from https://iotify.io/top-10-selection-criteria-for-your-iot-cloud-platform/

5 Ways To Measure Project Success - ProjectManager.com. (2015, September 28). Retrieved from https://www.projectmanager.com/blog/5-ways-to-measure-project-success

Corporate Image - Encyclopedia - Business Terms. (0000). Retrieved from https://www.inc.com/encyclopedia/corporate-image.html

Conseil gestion des identités et accès IAM - Identity and Access Management. (n.d.). Retrieved from https://www.harmonie-technologie.com/iam-identity-access-management

Certificats SSL et numériques GlobalSign. (n.d.). Retrieved from https://www.globalsign.fr/fr/

Nippon Telegraph and Telephone Corporation. (n.d.). NTT Home Page. Retrieved from http://www.ntt.co.jp/index_e.html

How to Plan a Promotional Event for Your Business - dummies. (n.d.). Retrieved from https://www.dummies.com/business/marketing/how-to-plan-a-promotional-event-for-your-business/

GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from http://www.planningplanet.com/guild/gpccar/risk-opportunity-monitoring-and-control

L'avenir des attaques distribuées par déni de service (DDoS). - Neotech. (2018, March 8). Retrieved from https://www.neotech-assurances.fr/lavenir-des-attaques-ddos/

Four ways to avoid IoT data fatigue. (2017, May 22). Retrieved from https://www.ibm.com/blogs/internet-of-things/iot-data-fatigue/

How to Train Your Users on Salesforce: Getting Started. (n.d.). Retrieved from http://pages.mail.salesforce.com/getting-started/train-your-users/

Principe de Pareto — Wikipédia. (n.d.). Retrieved November 11, 2018, from https://fr.wikipedia.org/wiki/Principe_de_Pareto

Méthode des 20-80 ou loi de pareto : comment faire ? (n.d.). Retrieved from https://www.manager-go.com/gestion-de-projet/dossiers-methodes/la-methode-des-20-80

L'assurance des pertes d'exploitation de l'entreprise. (n.d.). Retrieved from https://www.ffa-assurance.fr/content/assurance-des-pertes-exploitation-de-entreprise?parent=79&lastChecked=150

La responsabilité civile du particulier et son assurance. (n.d.). Retrieved from https://www.ffa-assurance.fr/content/la-responsabilite-civile-du-particulier-et-son-assurance?parent=74&lastChecked=120

About the Author

Thibault G.A. Kibler

Lille, France

🇫🇷

Thibault Kibler is a 5th year student at Iteem in France. It's an entrepreneurial graduate school providing a dual competence in engineering and management and a 5-year Master's degree awarded jointly by Centrale Lille and SKEMA Business School. He is also doing a double degree with Skema Business School: "MSc Project and Programme Management & Business Development". He made also some certifications: Prince2 Certifications, Agile certification and TOEIC certification (with a score of 955, equivalent to C1 English-level). He made an 8-months internship in London at Bouygues Construction UK in Linkcity, the real estate development subsidiary of Bouygues Construction. He was UK referent for IoT and create a brand-new offer for student housing. He was also member of several association during his studies, in the position of secretary. Because of these atypical experiences, he a strong experience in project management. He is above all someone ambitious, dynamic, organized and sociable. He has the ability to work in team, manage a long-term project and a strong capacity of adaptation.

Thibault lives in Lille, France and be reached at kibler.thibault@gmail.com.

You can have further information about his experience or contact through his Linkedin profile: https://www.linkedin.com/in/thibaultkibler/