IRDA

BLOCKCHAIN-BASED INCIDENT REPORTING DECENTRALIZED APPLICATION

INTRODUCTION

IRDA – THE INCIDENT REPORTING DAPP

IRDA is an information security incident reporting application

- It can be utilized as a reporting platform for organizations, for reporting their various information security incidents
- It is addressed towards a range of potential customers, including authorities and businesses, which can use the product both internally (i.e. reporting within the various departments of a single organization) or externally (i.e. reporting within a group of businesses, under a designated authority)
- Unlike other existing platforms, it is the first platform based on the blockchain technology and thus offers a range of additional benefits to users, which are presented in the next slides

SETTING THE STAGE

FACT: Organizations choose not to report their incidents!

Although virtually everyone agrees that information security incident reporting is beneficial to organizations (NIST, 2012; Gordon et al, 2003; ENISA, 2013; Gordon et al, 2015; Line & Albrechtsen, 2016; Gonzalez, 2005), reporting statistics show that very few incidents are actually being reported (IOD & Barclays Policy report, 2016; Symantec, 2016; Newman, 2018; Ipsos MORI, 2017; SentinelOne, 2016; ENISA, 2012)

Why? Mostly due to reputational risk

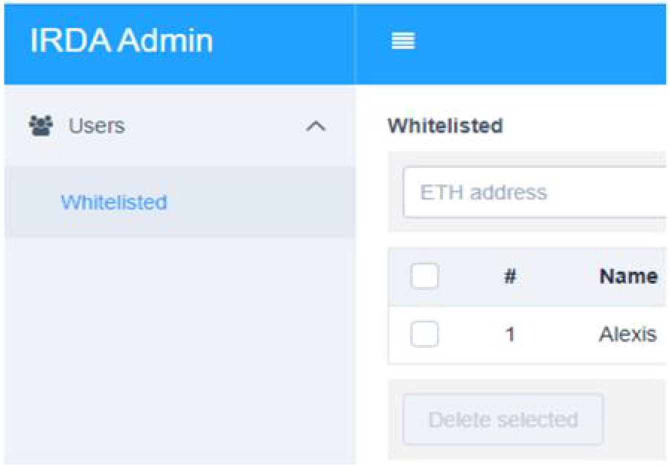
IRDA aims to motivate organizations to report their infosec incidents

How?

- IRDA utilizes the positive features of existing platforms, as identified by a thorough investigation of other commercially available reporting platforms.
- In addition, it offers several unique features, such as **reporting anonymity, lower cost, constant availability, immutability & transparency**.

So what?

IRDA was evaluated by different organizations in Cyprus. The results indicated a statistically significant improvement in the motivation level of users towards reporting incidents.



IRDA Admin

Users

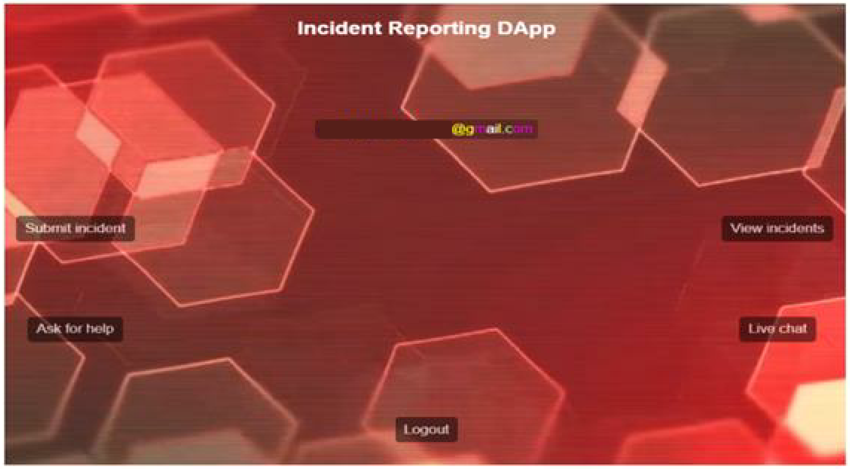
Whitelisted

Whitelisted

ETH address

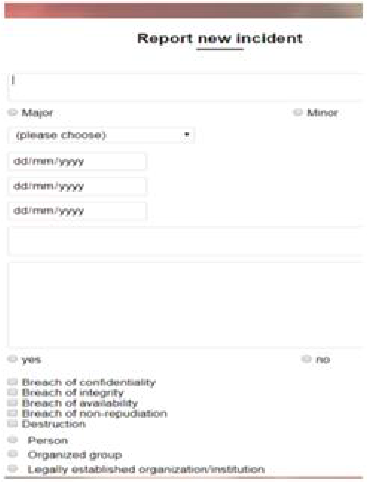
□	#	Name
□	1	Alexis

Delete selected



Incident Reporting DApp

[redacted]@gmail.com



Report new incident

○ Major ○ Minor

(please choose)

dd/mm/yyyy

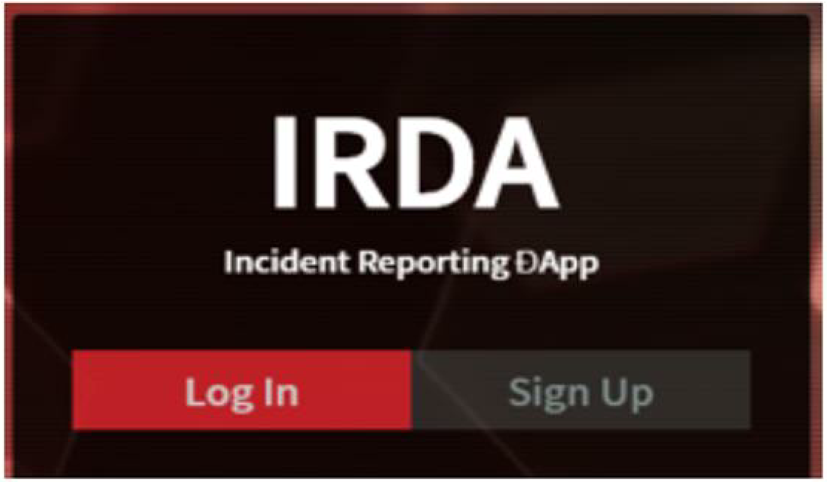
dd/mm/yyyy

dd/mm/yyyy

○ yes ○ no

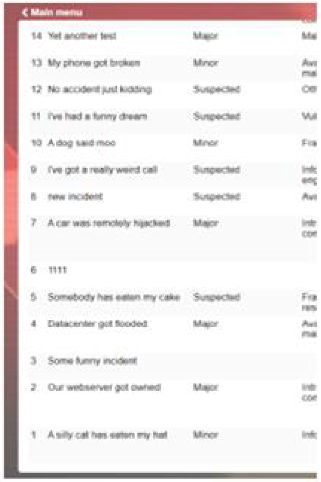
□ Breach of confidentiality
□ Breach of integrity
□ Breach of availability
□ Breach of non-repudiation
□ Destruction

○ Person
○ Organized group
○ Legally established organization/institution



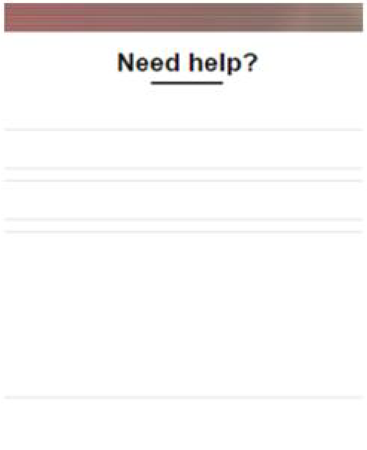
IRDA

Incident Reporting ÐApp

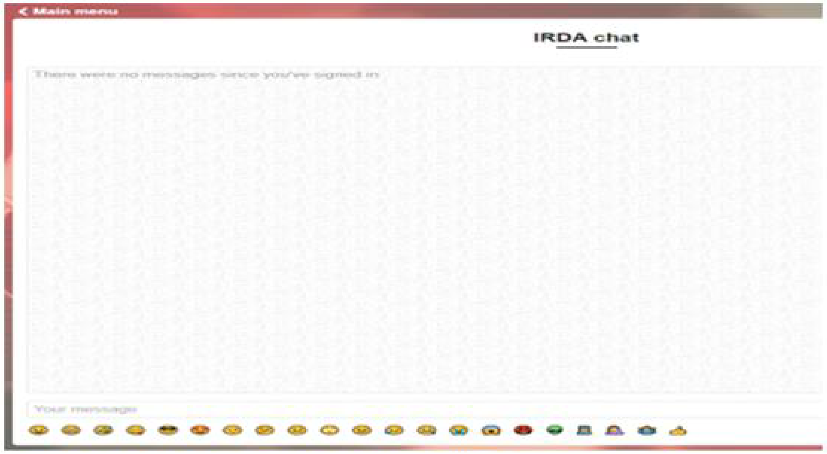


Main menu

14	Yet another test	Major	Ma
13	My phone got broken	Minor	Ava ma
12	No accident just kidding	Suspected	Oth
11	I've had a funny dream	Suspected	Vul
10	A dog said moo	Minor	Fra
9	I've got a really weird call	Suspected	Info eng
8	new incident	Suspected	Ava
7	A car was remotely hijacked	Major	Info con
6	1111		
5	Somebody has eaten my cake	Suspected	Fra res
4	Datacenter got flooded	Major	Ava ma
3	Some funny incident		
2	Our webserver got owned	Major	Info con
1	A silly cat has eaten my hat	Minor	Info



Need help?

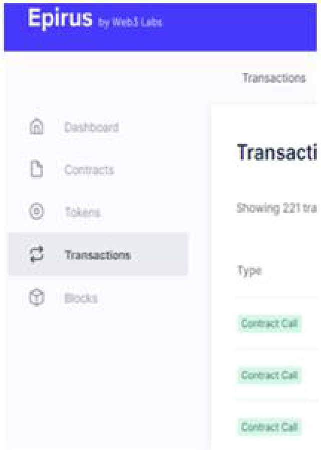


Main menu

IRDA chat

There were no messages since you've signed in

Your message



Epirus by Web3 Labs

Transactions

Transacti

Showing 221 tra

Type

Contract Call

Contract Call

Contract Call

UNDERSTANDING IRDA

The basics.

Blockchain technology

IRDA is built on “Quorum”,a permissioned blockchain implementation of Ethereum. Quorum utilizes a PoA type of algorithm, called IBFT, and supports privacy and confidentiality of both transactions and smart contracts. IRDA can be deployed in either a cloud or a local environment.

Interface

The front-end is built using HTML, CSS and JavaScript.

Functionality

Users of the platform can anonymously report an incident, view submitted incidents, chat in complete anonymity and ask the administrator for help.

Security

Communication between the users and the platform is encrypted. Multi-factor authentication is required for platform registration/ login purposes.

UNDERSTANDING IRDA

The basics

Easy to understand & use

The GUI has a clean design -it is easy to understand, use and navigate the reporting DApp. The internationally recognized “ISO 27035:2016”incident reporting template is utilized for creating the reporting forms, with a minor alteration: ISO’s proposed incident categories/ taxonomy have been replaced with the “eCSIRT.net mkVI” taxonomy, since the latter is endorsed by ENISA, its categories are universal and practical, and it is widely used amongst European CSIRTs.

Accessibility

The platform is easily accessible throughout the world (over the Internet), and only requires a Web3.0-capable browser and an Ethereum wallet.

Availability

Constant platform availability is ensured through the inherent characteristics of the blockchain technology.

Performance

A private blockchain implementation, as well as utilizing a less resource-intensive consensus algorithm (PoA/IBFT), increase the solution′s performance, efficiency and scalability. Quorum blockchain allows about 100 transactions per second, which is more than adequate for the expected use.

UNDERSTANDING IRDA

The basics

Anonymity

Anonymity of participants is ensured through Blockchain's inherent characteristics. Only the public key of each participant is publicly visible and no other identifiable data. However, the administrator of the platform can identify and match transactions and users, to enable smooth platform management.

Transparency & Immutability

Incidents are auditable and all participants can query the submitted incidents, through the use of a Blockchain explorer. Incidents are therefore both consistent and transparent. Incidents submitted over the platform are also immutable: they cannot be forged (due to one-way cryptographic hash functions).

Low cost

The cost of owning and operating the system is significantly less than similar systems.

Originality

This is the first, ever, incident reporting platform created utilizing the blockchain technology!

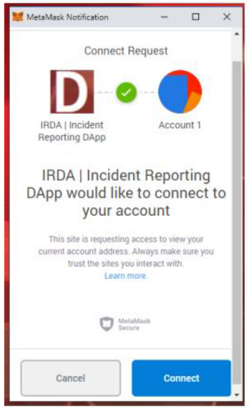
HOW IT WORKS

A simple example

The following example illustrates the flow of actions for logging-in to the platform, submitting an incident, viewing that incident in a list and tracing that incident through Epirus explorer:

1. Login to your whitelisted Metamask account.

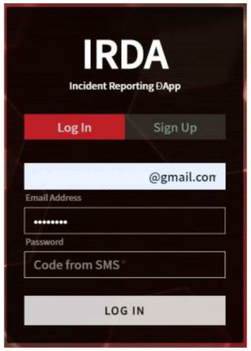
2. When prompted, allow IRDA to connect to your Metamask account.



IRDA | Incident Reporting DApp would like to connect to your account

This site is requesting access to view your current account address. Always make sure you trust the sites you interact with.
Learn more

3. Type your e-mail address and password and click login. When the SMS containing the OTP arrives, enter the code in the relevant field and click login once more

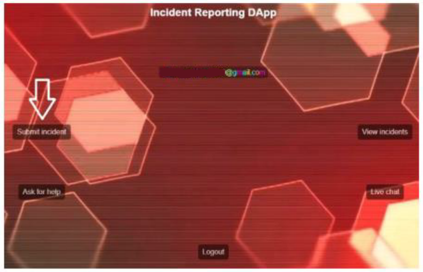


Email Address: @gmail.com

Password: ••••••••

Code from SMS

4. While on the DApp's homepage, select the "Submit incident button"

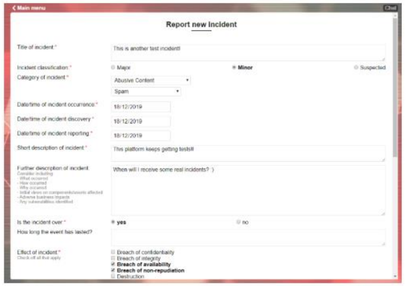


[redacted]@gmail.com

HOW IT WORKS

A simple example

5. Complete the report form with details of a mock incident.

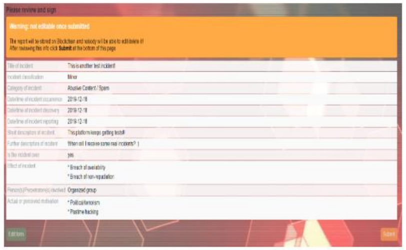


< Main menu

Report new Incident

Title of incident *	This is another test incident!
Incident classification *	○ Major ● **Minor** ○ Suspected
Category of incident *	Abusive Content Spam
Datetime of incident occurrence *	18/12/2019
Datetime of incident discovery *	18/12/2019
Datetime of incident reporting *	18/12/2019
Short description of incident *	This platform keeps getting tests!!
Further description of incident Consider including - What occurred - How occurred - Why occurred - Initial views on components/assets affected - Adverse business impacts - Any vulnerabilities identified	When will I receive some real incidents? :)
Is the incident over *	● **yes** ○ no
How long the event has lasted?	
Effect of incident * Check off all that apply	□ Breach of confidentiality □ Breach of integrity ☑ **Breach of availability** ☑ **Breach of non-repudiation** □ Destruction

6. Confirm the incident's details before final submission.



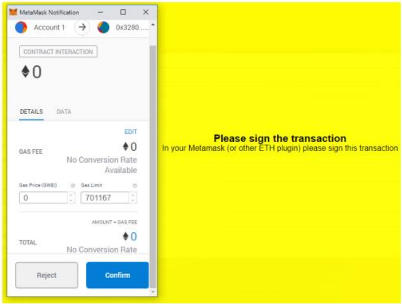
Please review and sign

Warning: not editable once submitted

The report will be stored on Blockchain and nobody will be able to edit/delete it!
After reviewing this info click **Submit** at the bottom of this page

Title of incident	This is another test incident!
Incident classification	Minor
Category of incident	Abusive Content / Spam
Datetime of incident occurrence	2019-12-18
Datetime of incident discovery	2019-12-18
Datetime of incident reporting	2019-12-18
Short description of incident	This platform keeps getting tests!!
Further description of incident	When will I receive some real incidents? :)
Is the incident over	yes
Effect of incident	• Breach of availability • Breach of non-repudiation
Person(s)/Perpetrator(s) involved	Organized group
Actual or perceived motivation	• Political/terrorism • Pastime/hacking

7. Sign the transaction with Metamask



♦0

GAS FEE ♦0 No Conversion Rate Available

Gas Price (GWEI): 0

Gas Limit: 701167

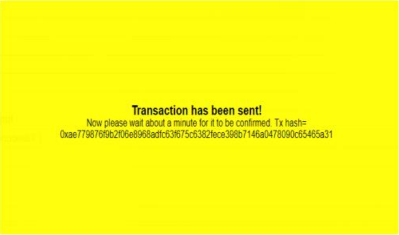
AMOUNT + GAS FEE

TOTAL ♦0 No Conversion Rate

Please sign the transaction

In your Metamask (or other ETH plugin) please sign this transaction

8. Transaction has been submitted!



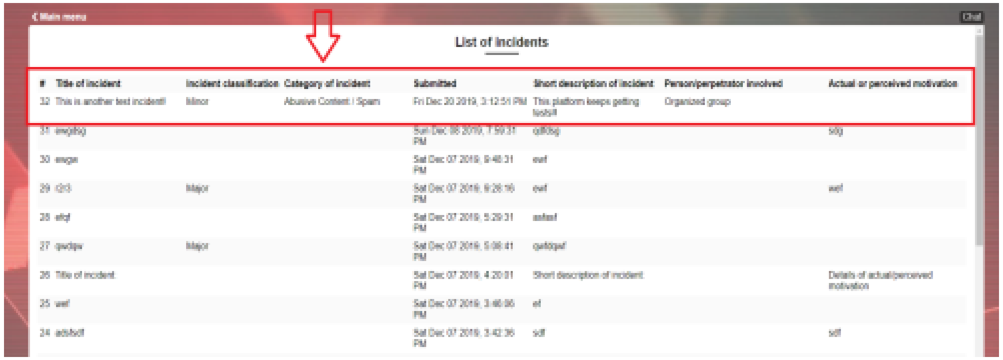
Transaction has been sent!

Now please wait about a minute for it to be confirmed. Tx hash=
0xae779876f9b2f06e8968adfc63f675c6382fece398b7146a0478090c65465a31

HOW IT WORKS

A simple example

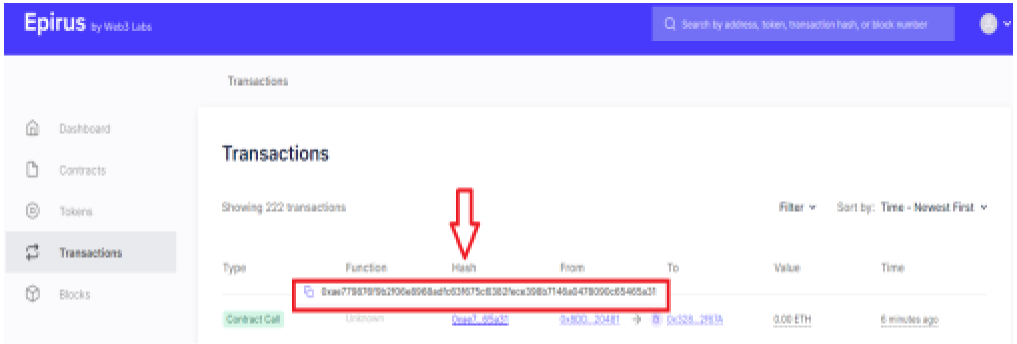
9. Transaction has been registered in incidents list



List of Incidents

#	Title of incident	Incident classification	Category of incident	Submitted	Short description of incident	Person/perpetrator involved	Actual or perceived motivation
32	This is another test incident!	Minor	Abusive Content / Spam	Fri Dec 20 2019, 3:12:51 PM	This platform keeps getting lostd!	Organized group	
31	ewgdsg			Sun Dec 08 2019, 7:59:31 PM	qdfdsg		sdg
30	ewgw			Sat Dec 07 2019, 9:48:31 PM	ewf		
29	r2r3	Major		Sat Dec 07 2019, 9:28:16 PM	ewf		wef
28	efqf			Sat Dec 07 2019, 5:29:31 PM	asfasf		
27	qwdqw	Major		Sat Dec 07 2019, 5:08:41 PM	qefdqwf		
26	Title of incident			Sat Dec 07 2019, 4:20:31 PM	Short description of incident		Details of actual/perceived motivation
25	wef			Sat Dec 07 2019, 3:46:06 PM	ef		
24	adsfsdf			Sat Dec 07 2019, 3:42:36 PM	sdf		sdf

10. Navigate to: blockchain explorer and confirm that transaction hashes match



Epirus by Web3 Labs
Search by address, token, transaction hash, or block number
Transactions
Dashboard
Contracts
Tokens
Transactions
Blocks
Filter
Sort by: Time - Newest First

Transactions

Showing 222 transactions

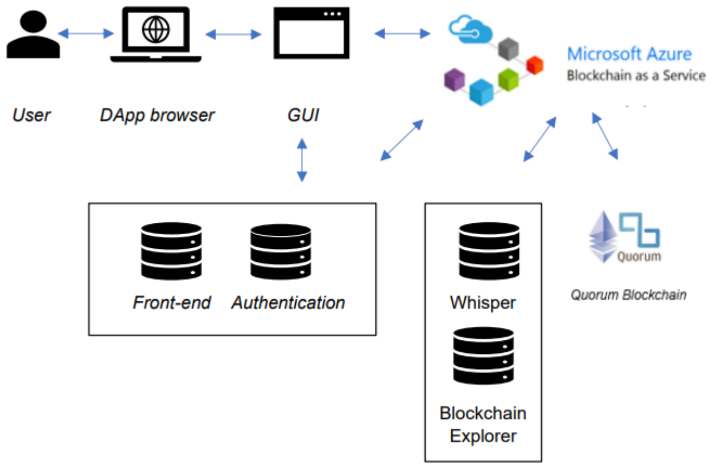
0xae7798f8f9b2f06e8068adfc63f675c8382feca398b7146a0478090c65465a31

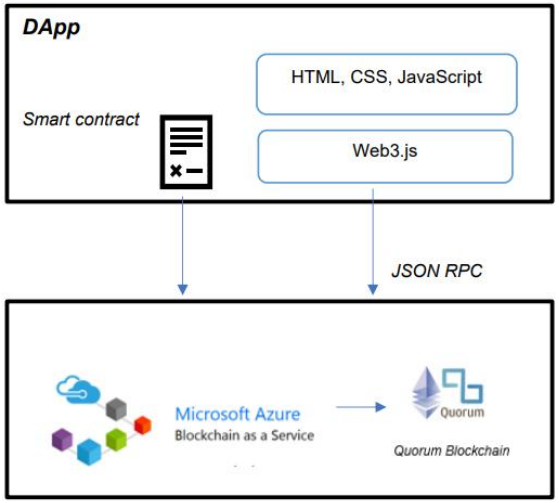
Type	Function	Hash	From	To	Value	Time
Contract Call	Unknown	0xae7...65a31	0x800...20481	0x328...2f61A	0.00 ETH	6 minutes ago

The incident has been successfully submitted on the blockchain!

HOW IT WORKS

DApp architecture & ecosystem (Cloud Version)





IN A NUTSHELL

Why would anyone want IRDA?

- A number of reporting demotivators, such as fears for negative publicity and increased reporting cost (Koivunen, 2010; Ahmad et al, 2015; Ruefle et al, 2014; Choo, 2011; Ahmad et al, 2012, Johnson, 2002; Metzger et al, 2011; Jaatun et al, 2009; Etzioni, 2014; HousenCouriel, 2018), were treated with embedding innovative features in the developed artefact, such as reporting anonymity, within a low-cost reporting ecosystem.

- Performance, efficiency, security, accessibility, the presence of social features (through the implementation of Whisper chat), as well as the solution's ease of use and understanding, were all positive features, which were identified through the evaluation of existing solutions, and were also incorporated in the developed artefact.

- The increased availability, immutability and transparency levels of IRDA can be regarded as further benefits of the solution.

- All the above provide the necessary added value, which may ultimately increase the motivational level of users towards the reporting of incidents.

- IRDA is addressed towards a range of potential customers, including authorities and businesses, which can use the product both internally (i.e. reporting within the various departments of a single organization) or externally (i.e. reporting within a group of businesses, under a designated authority).

- Furthermore, the platform could be of particular interest to the various CSIRTs and CERTs around the world (and especially within EU), which could evaluate its use over their current reporting solutions, built with conventional technologies. More particularly, the early assumption that European CSIRTs/CERTs could potentially be both customers of the decentralized platform, led to the integration and utilization of the "eCSIRT.net mkVI" incident taxonomy, since this taxonomy is endorsed by ENISA, its categories are universal and practical, and it is currently widely used amongst European CSIRTs.

REFERENCES

List of references appearing in this presentation

Ahmad, A., Hadgkiss, J., and Ruighaver, A.B, 2012, Incident Response Teams-Challenges in Supporting the Organisational Security Function, Computers & Security (31:5), pp. 643-652.

Ahmad, A., Maynard, S.B. and Shanks, G., 2015. A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), pp.717-723.

Choo R, 2011, The cyber threat landscape: Challenges and future research directions. Computers and Security 30 (2011) 719-731

ENISA, 2012, Cyber Incident Reporting in the EU: An overview of security articles in EU legislation [online] Available at: https://www.enisa.europa.eu/publications/cyber-incidentreporting-in-the-eu/at_download/fullReport

ENISA, 2013, Incident Reporting for Cloud Computing [online] Available at: https://www.enisa.europa.eu/publications/incident-reporting-for-cloud-computing

Etzioni, A., 2014, The private sector: A reluctant partner in cybersecurity, Geo. J. Int'l Aff., 15, p.69.

Gonzalez J.J., 2005, Towards a Cyber Security Reporting System – A Quality Improvement Process. In: Winther R., Gran B.A., Dahll G. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2005, Lecture Notes in Computer Science, vol 3688. Springer, Berlin, Heidelberg

Gordon L, Martin P. Loeb, William Lucyshyn, 2003, Sharing information on computer systems security: An economic analysis,Journal of Accounting and Public Policy, Volume 22, Issue 6, 2003, Pages 461-485

Gordon L., Martin P. Loeb, William Lucyshyn, Lei Zhou, 2015, The impact of information sharing on cybersecurity underinvestment: A real options perspective, Journal of Accounting and Public Policy, Volume 34, Issue 5, Pages 509-519

Housen-Couriel D, 2018, Information Sharing for the Mitigation of Hostile Activity in Cyberspace: Comparing Two Nascent Models, European Cybersecurity Journal, 4(3), pp.44-50

IOD & Barclays Policy report, 2016, Cyber Security: Underpinning the digital economy [online] Available at: https://www.iod.com/Portals /0/Badges/PDF's/News%20and%20Campaigns/Infrastructure/Cyber%20security%20underpinning%20the%20digital%20economy.pdf?ver=2016-04-14-101230-913

REFERENCES

List of references appearing in this presentation

IOD & Barclays Policy report, 2016, Cyber Security: Underpinning the digital economy [online] Available at: https://www.iod.com/Portals/0/Badges/PDF's/News%20and%20Campaigns/Infrastructure/Cyber%20security%20underpinning%20the%20digital%20economy.pdf?ver=2016-04-14-101230-913

Ipsos MORI Social Research Institute and the University of Portsmouth, 2017, Cyber security breaches survey 2017, version 4.5 [online] Available at: https://www.ipsos.com/sites/default/files/2017-04/sri-cybersecurity-breaches-survey-2017.pdf

Jaatun MG, Albrechtsen E, Line MB, Tøndel IA, Longva OH., 2009, A framework for incident response management in the petroleum industry, Int J Crit Infrastruct Prot, 2:26e37.

Johnson, C. 2002, Reasons for the Failure of Incident Reporting in the Healthcare and Rail Industries, in Components of System Safety, Springer, pp. 31-57

Koivunen E., 2010, Why wasn't I notified: information security incident reporting demystified. In:15th Nordic Conference in Secure IT Systems (NordSec 2010)

Line, M.B. and Albrechtsen, E., 2016, Examining the suitability of industrial safety management approaches for information security incident management, Information & Computer Security, 24(1), pp.20-37.

Metzger, S., Hommel, W., and Reiser, H. 2011, Integrated Security Incident Management-Concepts and Real-World Experiences, IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on: IEEE, pp. 107-121.

Newman C.A., 2018, The New York Times: When to Report a Cyberattack? For Companies, That’s Still a Dilemma [online] Available at: https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html

NIST Recommendations of the National Institute of Standards and Technology, 2012, Computer Security Incident Handling Guide, Special Publication 800-61, Revision 2

Ruefle, R., Dorofee, A., Mundie, D., Householder, A.D., Murray, M. and Perl, S.J., 2014, Computer security incident response team development and evolution, IEEE Security & Privacy, 12(5), pp.16-26.

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO Ltd to discuss these matters in the context of your particular circumstances. BDO Ltd, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO Ltd, a Cyprus limited liability company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

www.bdo.com.cy