Cybersecurity Trends

English Edition, No. 2 / 2018

VIP article: Airports at risk

iCyber-Security
SAFEGUARDING
YOUR DIGITAL WORLD

Central Folder | First thoughts after the GDPR implementation

WHAT MATTERS MOST
Cyber Security
Talks & Networking
GDPR/CYBER SECURITY TALKS
& NETWORKING

Contents

GDPR readiness consumed much of peoples time this year where will the next focus be

Author: **Norman Frankel**

Chairman, iCyber-Security

One of the benefits of being both editor of this magazine and an industry executive in a commercial cybersecurity business is the observation gained from real experience in the field. From my perspective, whilst the large story of the year so far has been the GDPR coming into effect on 25 May 2018, which clearly created some commercial opportunities, I have also noticed how slow the decision taking cycle has moved in the year to date.

Prior to the GDPR deadline in the earlier months of this year, even the easiest tasks of booking meetings and getting relatively simple legal documents reviewed became incredibly drawn out affairs. Some instances of tasks that would normally have taken days to close, became months to resolve whilst legal or technical resources tried to reach each other to clarify points between them. Post GDPR deadline, there was a brief catch up and multiple apologies for lack of availability, but this seems to have quickly reverted to the realization that other technology related projects which had been delayed or deferred now urgently needed attention, so once again we observe delays.

In this issue we have a number of articles looking at the subject of what next now that GDPR in enforceable. Whilst it should be business as usual there are still many areas that business still need to stay abreast of process, training and even implementation of projects to enhance compliance. The deadline came and went but in truth workloads still remain excessively high and grey areas of interpretation still exist. Against this backdrop demand for skills still outstrips the supply and I recommend reading the Money Talks article which sets out a raft of facts that only illustrates just how hard it is to hold on to your best resources.

Keeping your teams motivated, engaged, trained is a continual part of leadership but you can achieve significant boost and recognition by entering industry awards and allowing staff to attend conferences. Last year, I attended the Industry Awards which are promoted in this edition and wholeheartedly recommend both entering and attending the awards. For those who are London based attending the monthly CyberTalks networking events is recommended, details can be found on the website advertised in this edition. I regularly attend the Cybersecurity Trends conferences which is supported by the United Nations ITU. The next such conference will be held 11-13 September in Sibiu, Transylvania, details to reserve delegate places can be found on one of the adverts in this edition.

Whilst we have yet to have a high profile fine directly related to the new GDPR enforcement, we are starting to witness Next-Generation Cyberattacks. In April alone, U.S. defense and law enforcement agencies said they detected a new wrinkle in the latest attack methods. Instead of going after a vulnerable “backdoor” to a network, hackers were now targeting internet router devices.

Once the router is compromised, they can let their so-called “man in the middle” attack work its magic. As information flows back and forth between the user’s computer and the internet, the hackers monitor the information and collect what they want, or feed in new data to further confuse the victim.

These new cybersecurity attacks also point to yet another threat. Instead of a lone-wolf hacker sitting in a darkened room with a laptop, newer attacks increasingly appear in state-sponsored form. Analysts have taken to calling these “Generation V” attacks. That doesn’t mean that catchwords like “Russian hackers” or “North Korean attacks” are always accurate. But the attacks are becoming more sophisticated as the “black hat” hacker community encounters new cyberdefenses, then uses digital clues to more or less reverse engineer their way to a solution.

The scary part? As researchers at Check Point Software noted recently, these "large-scale and multivector mega attacks are using advanced attack technologies. Detection-only-based solutions are not sufficient enough against these fast-moving attacks. Advanced threat prevention is required."

All of this means continued spend in the Industry in the search for effective solutions. According to new data from analysts at Juniper Research, they believe global companies will boost their spending even further. They see investments in cybersecurity products and services rising by 33% over the next four years. By 2022, corporations will be spending more than $130 billion a year on this stuff. Why? Well, the threat isn't going away. For every hole in a network that gets plugged, hackers find another way in.

Another way to retain staff is by automating the task workload so that staff work on more challenging and interesting tasks rather than the menial, volume related tasks. Automation is an area of rapid advancement. In this edition we have excellent articles from Thales on automation in Airport Security and another article on why cyber criminals are probably winning. Looking back at history can often provide valuable lessons for the future and the article on the challenges that led to the fall of the byzantine Roman empire is worth noting for the communication challenges that arose, a situation that will undoubtedly happen in cybersecurity unless automation tools are embraced to free up time to get back to communicating between teams and business units across the Enterprise.

If we are to address complacency then it is Board and the Executives that need to set the tone of the culture to discuss and address these issues. Without an effective culture, collaboration even within the business will fail and breaches will remain common place. We invite you to join in the process and submit articles or suggestions for us to cover.

The goal of this publication remains to open up knowledge and information sharing across research and commercial activities, so providing a bridge between public and private dialogues, in an aim to help our world operate more safely giving the growing frequency of attacks that seem to endlessly get media attention.

If you would like to contribute articles or have suggestions for us to cover in future editions of the magazine, or even wish to purchase hard copy versions of the magazine to give to your customers, please do contact us via email at info@cybersecuritytrends.uk.

On our website http://www.cybersecuritytrends.uk you can also view publications in other languages /countries and purchase advertorials for future editions. ■

We are looking forward meeting you at Sibiu, September 13th and 14th, at the 6th edition of «Cybersecurity-Romania», a public-private dialogue platform on Central Europe. Have a nice summer!
https://cybersecurity-romania.ro
ITU

When does no news mean good news?

I wonder how many C-level managers went on this May Bank Holiday with a bit of trepidation. Not that the GDPR legislation has incidentally kicked in on a Friday ahead of a long weekend, but owing to the build-up of anticipation of what happens next.

Author: Vladlena Benson

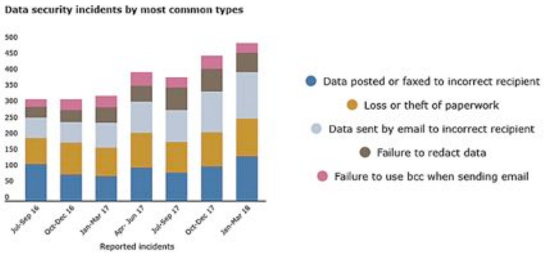
Organisations large and small have been dutifully following the updates from ICO. Now that the regulatory change is in the past what has happened since? It is yet to be seen who falls first victim of the GDPR sword. Yet, it is clear for CEOs that it is not a matter of how but a matter of when, a breach affecting their organisation will occur.

Research shows that cyber threats are growing in their complexity and sophistication. Well-funded criminal gangs, state sponsored attacks and those seeking to breach security to publicise an organisation's vulnerability and inflict reputational damage aim to compromise data.

We increasingly see attackers infiltrating organisations from within, thereby gaining access to their systems to understand their operations and plan the most effective breach. Those in cyber security roles agree that organisational security posture depends on people, more than on technical controls and threat countermeasures.

Recent analyses of cyber security threat landscape show that no industry segment is immune to cyber-attacks and the public sector tops the list for targeted security incidents[1]. This is largely attributed to the organisational cyber security culture and mindset of employees. In fact, the data on security threats published by ICO shows an increase in reported data breaches in Q4 2017-18, increased by 31% (from 74 to 97). The healthcare sector reported a rise in the number of incidents by 21%. These were largely due to the events caused by insider threats such as data being posted or faxed to the incorrect recipient, loss or theft of paperwork, and data emailed to the incorrect recipient. Similarly, a rise in reported incidents took place in the education sector by nearly 30% (from 96 to 127). The charities reported a significant increased incidents - up by 69% . These were caused by employee errors of data being emailed to incorrect recipients.

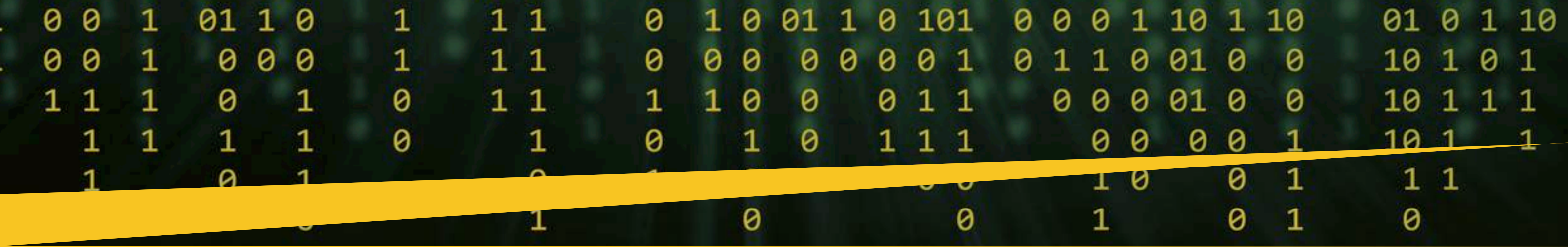
While no industry is immune to a data breach, the financial sector year on year experiences the highest volume of cyber breaches aimed at financial gain or espionage. According to the EY Cyber Security Survey (2018) organisations expect their cybersecurity budget to double in the next year. Another key insight from the survey is that only 12% of organisations are confident in their ability to detect a sophisticated cyber attack. The speed of technology developments present a particular challenge as organisations strive to keep up



Source: ICO Data Security Trends Q4 2017-18[2]

BIO

Professor Vladlena Benson leads the Cybersecurity & Criminology Centre at UWL and holds the role of Academic Relations and Research Director at ISACA LC. Prof Benson's research areas cover: information privacy; cyber victimisation; gender and culture differences in online behaviour; digital rights and the cyber vulnerability of young people. Her work also relates to religious orientation, digital behaviour and privacy on social media. Vladlena publishes widely in top ranked IS journals and has authored a series of books on cyber security. Professor Benson research has been covered by press, she writes for the Independent on cyber security and privacy issues. She is a strong advocate for increasing diversity. As a result of her work in this area, Prof Benson was recognised at the Women in IT Awards 2017 for helping the development of career opportunities for women in cyber security.

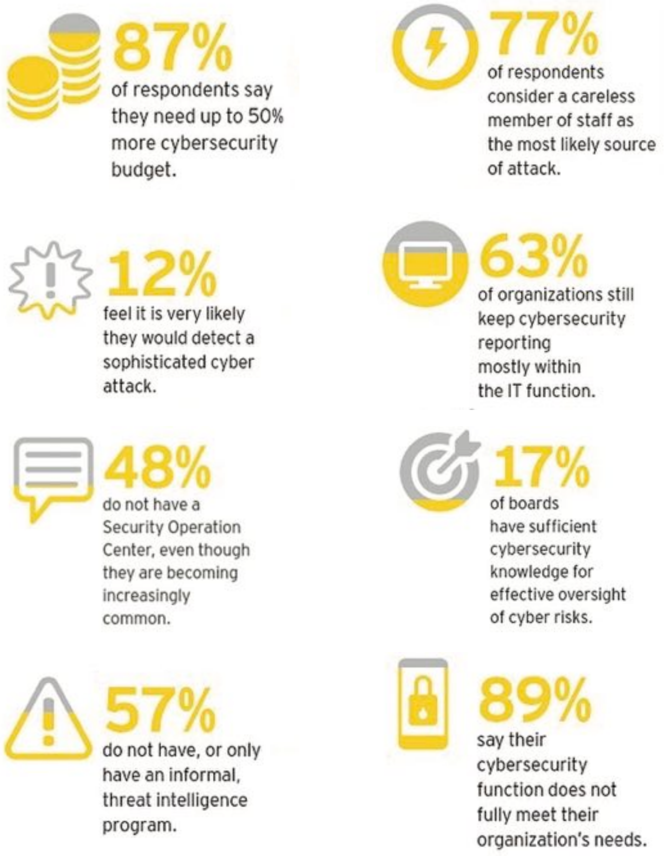


to date, whilst managing the evolving security risks which they must keep pace with too.

Irrespective of industry, the attack vector starts with social engineering the weakest link in the security chain. Over 77% of organisations state that a careless employee is the likely source of security incidents.

The threats imposed by employee errors are preventable in many cases. GDPR puts an extra level of responsibility onto organisations for incidents due to data being sent to incorrect address, for example. Insider threats can also be caused by malicious intent, although accidental loss of data has been reported to be the prevalent cause of data breaches in the last ICO report. GDPR highlights the importance for employees handling sensitive data to be appropriately trained and have a reasonably good understanding of cyber security practices.

It is yet to be seen if the GDPR will be effective in changing the way companies deal with data protection and whether the financial penalties that will be placed on companies make them more diligent. GDPR might encourage organisations to nurture behavioural change on the part of their employees. It is believed that most people want to do the right thing so by using the regulations, nudge and by leveraging the aspects of awareness, there will be positive changes in corporations and its employees working together to elicit secure cyber environments. ■



87% of respondents say they need up to 50% more cybersecurity budget.

77% of respondents consider a careless member of staff as the most likely source of attack.

12% feel it is very likely they would detect a sophisticated cyber attack.

63% of organizations still keep cybersecurity reporting mostly within the IT function.

48% do not have a Security Operation Center, even though they are becoming increasingly common.

17% of boards have sufficient cybersecurity knowledge for effective oversight of cyber risks.

57% do not have, or only have an informal, threat intelligence program.

89% say their cybersecurity function does not fully meet their organization's needs.

© Source : EY Report[3]

[1] Benson, V. (2017) The State of Global Cyber Security: Highlights and Key Findings. Learning Tree, London, UK DOI: 10.13140/RG.2.2.22825.49761
EY (2018) EY Global Information Security Survey 2017-18, EY Global. Available at: https://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18

[2] https://ico.org.uk/media/action-weve-taken/reports/2014676/data-security-trends-png.png

[3] EY (2018) EY Global Information Security Survey 2017-18, EY Global. Available at: https://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18

A publication

AGORA get to know! *and*

swiss webacademy web for business

edited by: iCyber-Security SAFEGUARDING YOUR DIGITAL WORLD

Copyright:
Copyright © 2018 Pear Media SRL,
Swiss WebAcademy and iCyber-Security.
All rights reserved.

Redaction:
Laurent Chrzanovski and Romulus Maier
(all editions)
For the iCyber-Security edition:
Norman Frankel

ISSN 2559 - 6136
ISSN-L 2559 - 6136

Addresses:
Bd. Dimitrie Cantemir nr. 12-14,
sc. D, et. 2, ap. 10, district 4,
040234 Bucarest, Romania
Tel: 021-3309282 / Fax 021-3309285

Griffins Court,
24-32 London Road
Newbury Berkshire, RG14 1JX, UK
+44 800 086 9544

www.icyber-security.com
https://cybersecuritytrends.uk/
www.icyber-academy.com
www.cybersecuritytrends.ro
www.agora.ro
www.swissacademy.eu

Author: Paul Guckian

Impact of GDPR on Biometric Systems

Many organisations and developers are worried about the impact of GDPR on biometric solutions, so let's explore the main security and compliance considerations involved. There has been rare, but poorly informed, advice given to customers that biometric systems cannot comply with the new legislation. But nothing could be further from the truth.

Background

Itis worth revisiting the meaning of "data", under the Data Protection Act, which means information that is:

a) being processed by means of equipment operating automatically in response to instructions given for that purpose,

b) recorded with the intention that it should be processed by means of such equipment,

c) recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

e) recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

BIO

Paul Guckian MSc, BSc,CISA,CISM,FBCS is Managing Director of DelaneyBiometrics, and holds 15 years of information security specialist experience, mainly in the financial sector. He is a certified IT Auditor and Information Security Manager with practical hands-on experience in all aspects of technology and Information Security Management. He is a guest lecturer in biometrics for universities such as Warwick and London City University. He has also served a Vice President of ISACA chapters and Chairman of the British Computer Society's special group in Information Risk Management & Assurance. You can connect with Paul via https://www.linkedin.com/in/paulguckian/

Therefore, raw images of biometric data is "personal data" by the definitions of the Act.

Raw biometric data may also meet the definition of "sensitive data" under the Act as it can reveal the racial or ethnic origin, or even the health status of the user e.g. facial recognition would usually involve sensitive data as it reveals race for example. Of course, additional security controls are required for sensitive data under the Act.

What is biometric data?

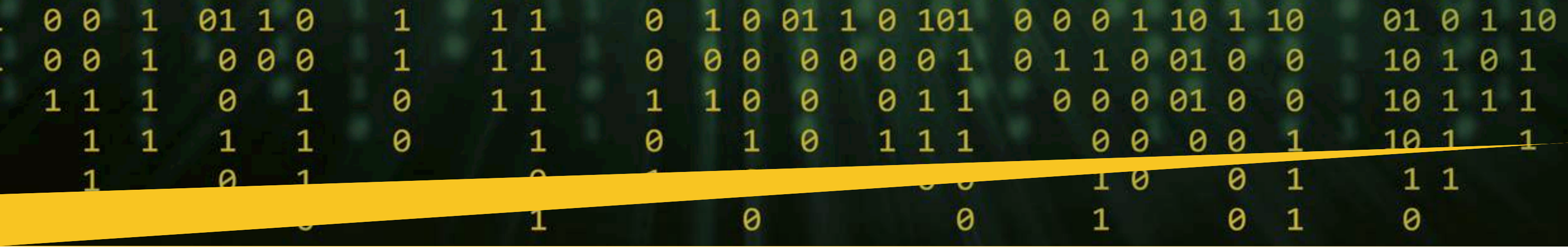
We should consider the two different kinds of "biometric" data which may be used:

#1 Biometric images are the raw picture of the biometric data (e.g. photo, fingerprint image), and is clearly personal data covered by the GDPR legislation. It can be readily encrypted to offer protection in storage or transit. This is the primary storage (along with templates) used by police and immigration systems, which can create confusion with the alternative approach used by commercial biometric systems.

#2 Biometric templates are hash values (same as password hash) representing the biometric patterns in numerical format. In itself, it is not normally considered 'personal identifiable information' as it is a one-way hash and cannot in itself be 'reverse engineered' to identify the user. This is the most common approach used by commercial biometric systems, which usually discard images to create a 'vendor lock' effect when selling their system and prevents migration to alternative systems.

But there are two data scenarios to be careful of when considering the impact of GDPR. Firstly, if another system has the raw data to re-create the template, and the data can be matched via an index, then it may meet the definition of personal identifiable information.

Secondly, all systems have to process a raw biometric image in memory to create or verify the biometric template so some 'personal identifiable information' is involved in all cases. Most commercial systems operate using this approach.



Delaney
ACCESS CONTROL
VEIN
Highly Accurate Identification
Central Enrolment & Reporting
Integrate with
Delaney
ACCESS CONTROL
FINGERPRINT
Entry & Exit Access Control
SDK for Custom Integrations
Scalable to 30,000 enrolled users
Delaney
ACCESS CONTROL
FINGERPRINT
IP65+ Rated Units for Outdoor Use
Wiegand Output for Easy Integration
Fast & Accurate Identification
Delaney
ATTENDANCE MANAGEMENT
FINGERPRINT
Fast & Accurate Identification
Work Codes for Custom Tracking
Push & Pull SDKs for Custom Integrations
Delaney
ATTENDANCE MANAGEMENT
FACE RECOGNITION
Easy User Enrolment on Units
Solutions for Tough Environments
Contactless, Fast & Accurate Identification

Impact of GDPR legislation

There remains a great deal of 'best practice' to be defined around the impact of GDPR and biometrics, and there still remains many conflicting views about the interpretation of the legislation with many 'consultants' erring on the side of caution. In relation to biometric data, the main principals of the new GDPR legislation are:

1. Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

Biometrics is no different to other forms of sensitive data, you must obtain permission to process the data. In most cases, biometric enrolment requires the users to comply with the enrolment process. Passive surveillance using biometrics is obviously an area where consent needs to be clearly communicated, probably via signage or other means.

2. Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Biometrics is the same as any other sensitive data in this regard.

3. Data minimization: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

There are clear business examples of where biometrics has exceeded the benefits of alternative authentication. Some examples include:

- Construction timesheets are up to 10% more accurate when biometric systems are used as it reduces buddy punching, ghost workers, and human error.
- Gym biometric access control reduce revenue loss by up to 5% for example, as it reduces card or PIN sharing. Ironically, the issue is highest in the lowest cost operators.

Therefore, business legitimately assess that biometric authentication is necessary to protect their commercial interests and staff safety matters, enabling these two sectors to operate on narrow profit margins. Other authentication options simply don't provide a genuine link to the system user andareopen to easier and possibly greater misuse or fraud.

Storage of raw biometric images may be considered excessive or even unnecessary, when biometric 'templates' would have sufficed, so careful consideration needs to be given to the storage approach used.

4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date

Biometrics is the same as any other sensitive data in this regard.

5. Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

One point which is often raised is that biometric data must begin in a raw format before it is converted into a 'biometric template'. Clearly, some raw image processing is necessary to turn the image into a template. Higher security biometric sensors carry out encryption and/or template creation on board the hardware module and also offer hardware identification controls to restrict connection of unauthorised hardware thereby managing the risk effectively.

In terms of risk assessment, the same risk scenario exists with key logging for example, in that the system input data can be intercepted before it actually reaches the system. This isparticularly relevant in the area of cybersecurity, so therefore a similar risk assessment approach may be taken with biometric inputs.At the point a user is presenting themselves to a biometric system, they are consenting to do so, which makes its similar to entering data on a web page.

6. Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Biometrics is the same as any other sensitive data in this regard.

7. Accountability: The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.

Biometrics is the same as any other sensitive data in this regard.

Impact on Biometric Systems

The benefits of biometric authentication are significant for many organisations, as it is both a convenient and secure form of individual authentication. Biometrics are the only authentication mechanism which truly linksactual users (rather than their security identity) to their specific actions. It is also the only authentication method to offer true de-duplication of user records, hence its use in voting systems.

Native biometric data has the same 'personal identifiable information' data classification as any other personal information such as Name, Date of Birth etc., and in many cases comes under sensitive data it would identify the race or ethnic origin of the person.

Some of the arguments against biometric data is that it cannot be changed, but this is similar to 'Date of Birth' and other sensitive personal data in this regard. Biometric templates are 'hash values' and don't directly identify users, and these stored values can be changed by using an alternative algorithm approach. Indeed some system that detect an exact 'replay' of biometric data reject the input as its is statistically unlikely that you would have a mathematically perfect match.

The use of biometrics may be quoted as 'excessive' or 'unnecessary' by those objecting to its use. If construction timesheets are up to 10% more accurate when biometric systems are used and gym biometric access control reduce revenue loss by up to 5-10%, then the use of biometric systems has real and genuine value to businesses. This enables these two sectors to operate on very narrow profit margins. Business legitimately assess that biometric authentication are necessary to protect their interests, as other options simply don't provide a genuine link to the system user, are less convenient and potentially more open to fraud.

In biometric systems, the 'personal identifiable data' is being processed when the biometric data (e.g. fingerprint) is captured by the scanner to when it's converted into a template or used for authentication seconds later. Except in the case of passive surveillance, raw biometric data has to be 'offered' by the end user so therefore by definition has their consent. During the first phase, the raw biometric image is processed by the scanner and within seconds it is using the biometric template (secure hash value). The data is processed like any other data between the client and server thereafter, such as the use of web browsers. In this regard, it's no different than typing your date of birth or name on a web page before it's securely processed by a web application. There is a moment when the data is exposed on the screen before it is then secured.

Conclusions

The use of biometric data is a well established mature authentication mechanism. It cannot be considered 'excessive', as there are very sensible and commercial reasons to require its use (de-duplication, anti-fraud, accuracy, convenience). Just as your bank requires a 3-5 year address history to identify you and detect fraud, a biometric system may be a legitimate requirement for customers or internal users. If an alternative authentication is offered, then this can mitigate the feeling of 'compulsory' biometrics, but this can quickly undermine the security of the biometric system, the more secure approach is multi-factor biometric authentication.

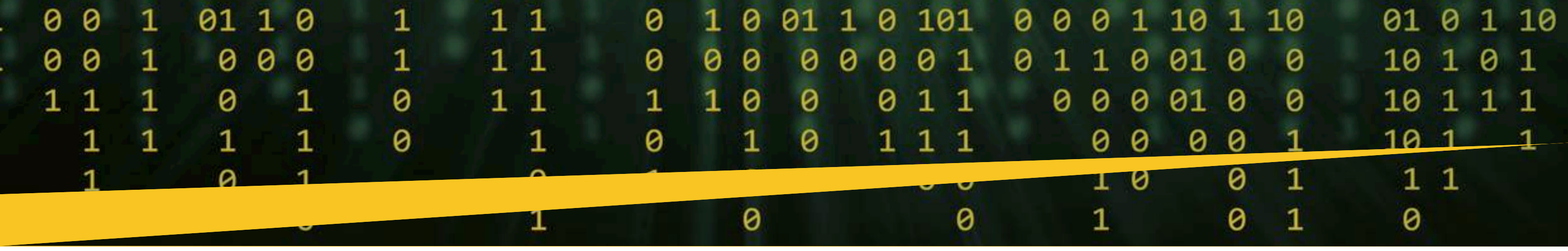
Passive biometrics is probably the one area that is affected, but the millions of CCTV cameras in use in the UK will need to consider the impact of GDPR. In some sectors like pubs, CCTV is a licensing requirement, so it will take some time for the legislative impact to be established in case law and fully understood consistently.

Biometric data can be a sensitive subject for some end users. There are links with police and immigration systems which can generate emotive meanings for end users. However in law, biometric data with regards to GDPR legislation, is just another form of (sensitive) data. The ICO has issued specific guidance on the use of biometrics for children for example.

Biometric enrolment should be subject to the same consents and approvals as any other sensitive data. Raw biometric data is personal data in the case of risk assessment categorisation, and may be sensitive data. Biometric templates may or may not be personal data depending on system design. Therefore, the design of the system needs to be carefully understood to correctly assess the impact. The use of biometric data is not directly threatened by the GDPR legislation, and any organisation which designs its procedures to comply with the GDPR legislation should include 'biometric data' in its risk assessment in the same manner as other sensitive data. ■

About DelaneyBiometrics

Since 2003, DelaneyBiometrics has been the UK & Ireland's leading specialist biometrics distributor. We operate the UK's only biometric experience centre at High Wycombe, about 20 miles from London Heathrow airport. The centre provides live demonstrations of biometric authentication solutions such as single sign-on, access control and attendance management using a range of modalities including fingerprint scanners, facial recognition, iris recognition, vein scanning and voice recognition. You can contact us via www.delaneybiometrics.com or (01342) 810 810.



GDPR: What comes next?

So, the 25th May has passed, the biggest change to data regulations within our millennial era is now in place. For the past two years companies left, right and centre have been frantically changing their data protection policies, following the ICO advice and getting their house to make sure they are GDPR compliant. But what's next for this mammoth beast? What's going to happen within the digital world?

Author: Jonathan Stock

For those who have been hidden under a rock for the past two years, GDPR (General Data Protection Regulation) is a regulation in EU law on data protection and privacy for all individuals within the European Union, or who have data held within EU states. It replaces the out-dated Data Protection Directive and brings all of the policies and practices in line with the modern era of working. Much like Arsene Wenger replacing the drinking culture of Arsenal FC footballers with an athletic breed of training schedules, GDPR is there to help individuals take control of their data and be safeguarded within the digital age.

Since May 2016 the ICO has been gearing up to the 25th May 2018 for the GDPR regulation to come into effect. They've sent out advice and guidelines based around awareness, information you should hold, communicating your privacy policy, the rights of individuals, subject access requests, how to correctly process personal data, (now let's take 2 seconds to breathe before you pass out at the end of the sentence!) what quantifies consent for individuals, what to do with data breaches, data protection impact assessments, establishing a company's data protection officer and clarifying a company's international borders.

Simply put, if you haven't done this yet as a company you have a lot of catching up to do and a very short window to do it in. The ICO gave the 2-year preparation window to help companies get their data policies up to scratch; they don't want to start punishing companies, they want everyone to be compliant. From now on they will be taking a hard line with organisations and individuals that don't abide with GDPR; with potential fines up to €20 million or 4% of the company's annual global turnover, this is something they are keen for everyone to follow.

BIO

Jonathan Stock heads up the IT Security recruitment team at IntaPeople and works with companies of various sizes helping them to source talent across the UK. He is part of the South Wales Cyber Security Cluster, helps to put on events and also regularly contributes to online security magazines. He has a genuine interest in security and the effect it is having in our globalised world.

LinkedIn – https://www.linkedin.com/in/jonathan-stock-112a2853/

Twitter – https://twitter.com/JonathanStock86

KEEP CALM AND COMPLY WITH GDPR

There's a bit of background on GDPR; the monster that has encroached on everyone's lives in some way over the past 2 years. In the lead up to the date companies were mailing out consent / marketing emails to the majority of their database, trying to get consent to keep their data on file or consent to continue marketing to them. From my understanding, even if you didn't reply at all, companies should put you on their opt out lists as they haven't given consent to be opt in. If you didn't reply they should probably start waving bye bye! Nice little rhyme that…!

So what's next for GDPR?

From my point of view, it's probably going to be like Y2K; all the leg work and scurrying around is over, now it's just time to crack on and make sure the changes your company has made are sustained moving forward.

(Continues on page 11)

Proving your credentials – A potentially more secure future via Blockchain

Author: Daryl Flack

Your digital identity is the gateway to your data, and increasingly, this includes most facets of your everyday life. Whether it's your social media accounts, your bank details, your chat history or your shopping habits.

With so many accounts to manage and protect, maintaining constant access across multiple devices whilst keeping them all secure can be an increasingly complex task.

BIO BLØCKPHISH

Co-Founder & CIO, BLOCKPHISH
Ever since watching the film War Games in the early 1980's, Daryl was fascinated by the fact everything from school grades to military mainframes could be hacked.
This interest later became the basis for his passion to design secure platforms and systems for everything from community and e-commerce sites to Government and defence systems.
Over the past 16 years, this passion has evolved from designing robust system to helping both companies and people with their security challenges.
Twitter: @blockphish
LinkedIn:
https://www.linkedin.com/company/blockphish/
https://www.linkedin.com/in/darylflack/

With data more valuable than ever, these large collections of personal data are very attractive targets to criminals as are the credentials that unlock access to them.

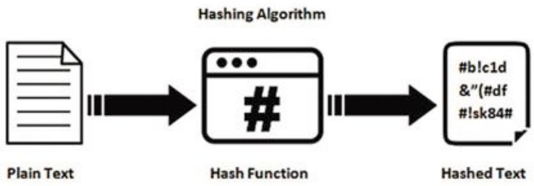
Recent breaches show that vital personal information for vast numbers of people, often give hackers the key information they need to unlock access to even greater volumes of data or even worse, the ability to use a victim's identity.

So, what is the answer? Well, one answer gaining more credibility is to move the control of your identity from the companies that you consume services from, to individuals themselves, giving them the ability to control which aspects of their personal what data is used and when.

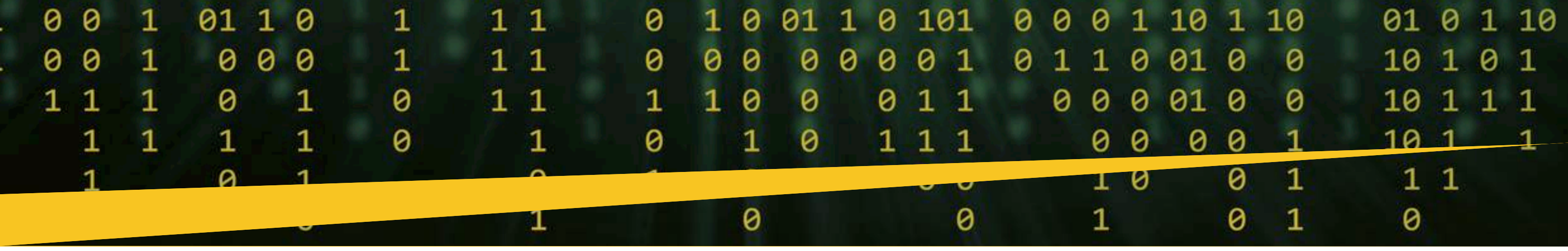
To achieve this, you effectively need two things:

1. A way to prove your identity without divulging sensitive data
2. A way for services that you want to consume to authenticate you

To achieve the first, a simple and well understood approach can be used, hashing. Hashing is a mechanism used to generate a value from some existing information, using a mathematical function. If you were to change any of the original information and rerun the hash, it would provide an outcome completely different to the original hash.



Hashing is also a one-way function due to the way it is calculated so reversing it is not a trivial task. This therefore makes hashing a very convenient mechanism for hiding underlying data whilst ensuring it hasn't been changed in transit.



By utilising the above approach, you could hash the details of your identity and use the hash for authentication without revealing the personal data you used to create it, thereby maintaining the security of your data. Obviously, this assumes that the original personal data or identity the hash was generated from was adequately verified before the hash was created but this should not prove a complex task. We do this all the time with physical forms of ID such as passports and driving licenses.

However, creating a hash of an identity is not very useful if no one can use or interact with it. This is where a secure, ubiquitous, transactional system is required and a relatively new one is showing signs of being a good candidate.

Blockchain allows parties to transact securely without any third-party involvement, removing the need for complex (and sometimes costly) intermediaries to enable direct peer-to-peer interaction.

Each transaction is independently verified before it makes it on to the Blockchain ledger which means there is no centralised authority and thereby no single point of failure. This decentralisation is one of the potential benefits from a security perspective. Once the data has been entered in to the blockchain, no one can change it and so it provides verifiable proof of the integrity of the transaction. It also removes the need for human involvement thereby eliminating the need for passwords.

By combining a digital identity verification service with the decentralised blockchain principle, a digital ID can be created from either all or parts of your ID which can then be used to transact for services. For example, you could just authorise the hashed part of your ID that provides your age for purchasing alcohol or just your address for having goods delivered to your home from a courier.

With both a verified ID to authenticate against and a secure platform to transact with, there is no need for your personal information to be disclosed, you just need to set the conditions of what you want to authorise, when you want to authorise it and to who.

Whilst large scale adoption and interoperability of verification services and Blockchain is yet to take place, the ability to build services in to blockchains is becoming more ubiquitous and some companies are already selling ID services in this area.

Therefore, don't be surprised if you start to see accelerated progression towards self-managed digital IDs soon, especially with GDPR now in place. ■

GDPR: What comes next?

(Follows from page 9)

Mainly businesses should be thinking about their processes and how they can quickly share the data that they hold if requested by another individual or organisation. Companies will inevitably get more enquiries on the subject so it's all about handling and triaging these enquiries in a compliant manner which meets the regulation. If someone asks for access to their data you can't bury your head in the sand, you can't try to palm them off and forget they exist, you've got to comply and make sure you (as a company or an individual) are acting in the correct way.

As well as making these changes within EU Law, us lucky lads and ladies in the UK have to think of life post-Brexit. Firstly, apologies for mentioning two buzzwords (GDPR and Brexit) in one article but it's pretty important.

When we leave the EU, as part of the agreement we will be covered by EU law for 2 years; a sort of safety blanket if you will to help the transition. The UK Government now needs to create a law to cover everything within GDPR and the previous Data Protection Directive, to make sure we create something that is better, more secure, and more transparent than everything else. Then we, as a country, can freely exchange data with any country in the world.

In terms of GDPR casualties, I am sure many in the industry have opinions on which company will be the first to get a slap on the wrist from the ICO. I'm happy to start a sweepstake to accommodate this (but don't worry your data will not be used for anything other than this!) but ultimately within the next few months, post-GDPR, I am sure there will be plenty of stories in the press of breaches and figuring out how much compliance there is with GDPR in general across different industries.

If, after reading this you feel like you still need to get up-to-date with GDPR, then I highly recommend using the ICO and NCSC websites for information on what to do; they've got helpful guides and one-stop shops to show you how to become compliant. There are various companies who can help and offer some good advice (there are also some companies to avoid; I have heard horror stories where companies were advising the wrong date for GDPR…!) so feel free to reach out and I can make introductions.

Ultimately, GDPR is the biggest change to our data protection laws for quite some time. The move will help bring legislation into the new digital era and provide a bigger safeguard. If you arenot compliant you may have missed the deadline given, but it's never too late to change for the better. ■

A Cyber Security strategy to mitigate risks in complex and critical environments: the case of airports[1]

Authors: Samuele Foni and Luca Ronchini

Samuele Foni

Luca Ronchini

Abstract

Airports are critical and complex systems that represent an excellent case study for establishing a flexible and reusable cyber security framework for risk mitigation. A complex system is made up of interacting components (agents) that adapt their behavior overtime in reaction to changes with respect to their environment and to each other [3]. Within such infrastructures, absolute security does not exist, because it is unfeasible to protect the whole system against every possible threat that might occur, especially those due to human errors and IT cyber degradation events. However the right use of cyber security best practices, the adoption of a cyclic and stratified Top-down investigative approach, the non-stop review of operating processes, the exertion of an appropriate cyber resilience plan, and the admission of staff training courses in order to raise employee awareness on security issues, can limit the likelihood of triggering events that could cause damage to people, structures, and assets, preventing them from experiencing economic losses or reputation damages. The only viable solution is to establish a never ending procedure of cyber security improvement, providing a suitable trade off in terms of protection and usability, with the aim of merging it with common everyday practices, avoiding any kind of impact on the company mission.

In this investigation we will assess airport security using an emergent vision, inspired by the paradigms of stigmergy and swarm intelligence, in order to establish a capillary control of complex systems endowed with a chaotic, interconnected, sociotechnical and strongly dynamic-dependent nature, both from a physical and operational point of view. This research has the aim to minimize the risk related to airport weaknesses taking advantage of an analytical complex systems approach and of a continuous improvement in cyber resilience.

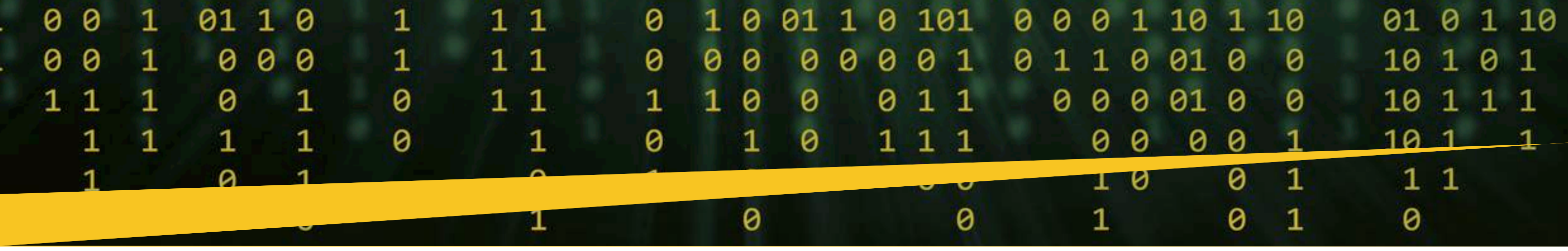
BIO

Samuele Foni is a Cyber security System Engineer at Thales Group, involved in the research activity related to the SESAR2020 project.
samuele.foni@thalesgroup.com

Luca Ronchini is a Security Expert at Thales Group with a grounded experience in IT infrastructures and management of complex architectures, networking and network security.luca.ronchini@thalesgroup.com

Introduction

A *complex system* is any system whose evolution cannot be explained starting from the analysis of all the parts and the inputs that make it up. Conversely, a *critical system* is a system that must operate with a high level of reliability because its failure can cause serious damage to things, environment and people, often irreparable. Moreover another category of system must be taken into account, that of *complicated systems*, whose nature can be formalized as an intricate set of devices, protocols and procedures that are difficult to setup but which provide an absolutely predictable output. Airports are complex, critical and complicated systems. For this reason they represent an excellent testbed to face the development of a cyber security framework that works efficiently in such contexts. Moreover, within the



Air Traffic Management (ATM) community, there is strong interest in cyber security, as demonstrated by the various research areas of the SESAR2020 project. Especially in view of the growing number of interconnections between landside and airside systems expected in the development of the next generation airports [1].

This paper starts by providing a brief explanation of the limitations of using a traditional approach to cyber security when dealing with a complex system. Section III discusses about a prototype of cyber security framework for securing critical and complicated systems. Section IV contains directions for a theoretical example of the use of artificial intelligence techniques applicable to the cyber security framework described above, with the aim of making it more suitable for the protection of complex systems. Finally, our conclusion follows in Section V.

The limitations of traditional cyber security approaches in complex environments

Cyber attacks are like pathogen infections and, as such, they can be the outcome of a combination of circumstances rather than the result of the exploitation of a standalone vulnerability. In other words, it is the "whole" of the circumstances and actions of the attackers that cause the damage [2]. The problem is that traditional strategies like the *divide et impera* provide a strong focus on causality, but a complex system cannot be analyzed merely by understanding its parts [6]. This is confirmed by the fact that despite the use of multiple layers of defensive cyber security approaches, cyber attacks still occur. In fact, the use of traditional techniques leads us to a paradox, as Turing has shown in his Halting problem of Undecidability, it is not possible to build a machine that can test another in all its cases, but to find all the faults and the vulnerabilities stored on it, we need to test the system totally. That is the reason why it is necessary to use a holistic approach in order to evaluate the emerging behavior of complex systems.

How to build a framework for risk mitigation in complicated and critical environments

Despite the limitations highlighted above, traditional cyber security techniques are at the heart of system security and, as such, they should not be omitted. In fact, an appropriate use of these techniques is enough to guarantee a high protection profile of critical and complicated infrastructures. In particular, if the set of cyber security best practices becomes part of the ongoing development of an infrastructure, it is possible to drastically reduce both the risk factor and the number of exploitable carriers by cyber threats through the adoption of a flexible, dynamic and well-structured framework.

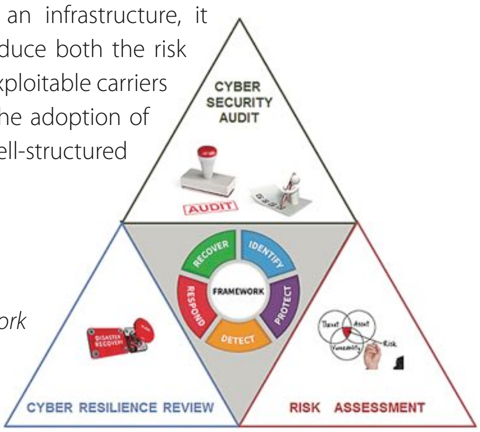


Fig. 1 *Cyber security framework for securing critical and complicated systems set as never ending process.*

The research work related to the safety of critical airport systems, carried out within the SESAR2020 project, was particularly fruitful in this context, maturing the development of a cyber security framework able to manage in time continuity the securing of critical and complicated systems, using a Top-Down analysis approach. This framework exploits the concepts consolidated by the main cyber security standards to actively intervene into the identification, protection, detection, response and recovery of all threats related to the cyber world. The construction and updating of these procedures, however, is the result of periodic investigations, reported in Fig. 1 by three main logical blocks: *Cyber Security Audit, Risk Assessment* and *Cyber Resilience Review*. The level of detail involved in these activities grows up as we go down from the top to the bottom, following a pyramidal structure. Performing these three tasks periodically means improving the status and capabilities of the framework under every aspect, providing new scenarios to consider, new countermeasures to be taken, new threats to be assessed and so on, establishing a continuous progress on the needs of the whole infrastructure.

a. Cyber Security Audit

Starting from a vision of the highest level, in which we are exclusively aware of the system as a whole without its parts, it is possible to undertake the cyber security audit task. Firstly, questionnaires are carried out to both operators and infrastructure managers in order to achieve the following purposes:

- to assess whether the best practices of cyber security are applied appropriately;
- to enumerate the sub-systems that make up the infrastructure;
- to identify the operational processes already in use;
- to increase the level of awareness on the risks related to cyber security to all the staff involved;
- to list the points of access to the system both a physical and digital point of view.

Secondly, a first analysis of the obtained results must be carried out, followed by an increasingly more detailed survey aimed at identifying the *Primary Assets* of the system on the one hand, and both the access control systems and the perimeter defense devices on the other hand. This information will constitute the input parameters of the tasks that follow, respectively the Risk Assessment and the Cyber Resilience Review. Meanwhile the scenarios emerged from the output of the Cyber Security Audit task become part of the framework.

b. Risk Assessment

Historically, the objective of the Risk Assessment activity is to carry out a risk evaluation. The list of identified primary assets is input and a first priority measure is provided. Subsequently we associate each asset with the subsystems and the devices that may have a certain influence on it. Going even further into details, we identify the vulnerabilities related to all the support devices through the activities of Vulnerability Assessment and Penetration Testing. Finally we carry out an assessment of the risks associated both to the vulnerabilities and to the threats previously identified, providing a measured probability and determining their degree of acceptability. From this task, patch management operations, code reviews and targeted hardening processes will emerge, and these will strengthen the security measures used by the framework.

c. Cyber Resilience Review

Starting from the analysis of the configuration files of the access and perimeter defense devices, it is necessary to verify the level of resistance and robustness of the whole infrastructure. This task is called Cyber Resilience Review. We proceed with a thorough check of the countermeasures in place, as well as the functional testing of the detection, alarm, notification and prevention systems. Then move on to the verification of the disaster recovery plan which is used, trying above all to evaluate its efficiency, effectiveness and degree of redundancy. Finally, a deep control of the response systems must be carried out, examining both their flexibility and reaction times. An audit of this type should make the system able to "learn" from its mistakes, equipping the framework with new countermeasures, new operational processes and new response techniques that shape its evolution.

How to increase reliability by including a complexity-based approach into the previous cyber security strategy

The approach described above is perfectly able to manage a critical and complicated system, since it allows to reduce the following issues:

- human or procedural errors;
- risk vectors belonging to the system;
- number of successful attacks.

Nevertheless this scenario is not enough to manage a complex system in the best way. Moreover, nowadays there are no sophisticated techniques that allow to manage complex infrastructures automatically. It is in this context that the idea of introducing artificial intelligence techniques can be applied to cyber security, with the aim of further reducing the possibility that attacks on the system are carried out, not because it is essential to protect a complex system, but mainly because these systems are critical and, as such, must be protected with the help of any means.

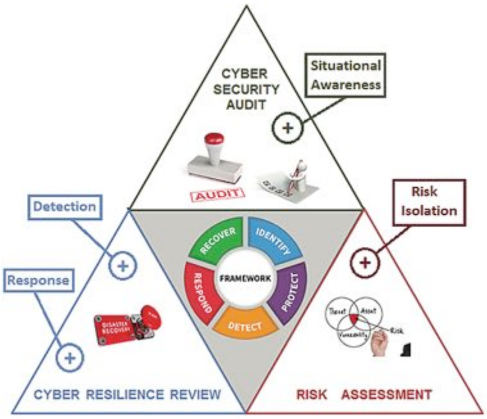


Fig. 2 *Cyber security framework with the addition of the main improvements introduced by the adoption of an artificial intelligence approach for securing complex systems.*

In the literature, it is possible to identify some examples of artificial intelligence application to cyber security, mostly theoretical, with the aim of making improvements to one or more of the following aspects [5]:

1. Detection;
2. Situational Awareness;
3. Risk Isolation;
4. Response.

Taking into consideration the framework presented in Fig. 1, we could think to equipping it with all these features, thus obtaining the diagram shown in Fig. 2. At a glance, it is clear that, two of the most immediate improvements deriving from artificial intelligence applied to cyber security insist on the activity of Cyber Resilience Review. This result is not the result of chance, in fact, the Cyber Resilience represents the versatile and adaptive engine of the entire infrastructure and, as such, is a complex system itself. Improving Cyber Resilience Review activity is the key to optimize the cyber threat mitigation process, taking advantage of a complex systems management approach. For example, we can consider biological systems, which represent an excellent sample of complex system, whose strength is characterized by their robustness to disturbances and changes. If this concept is abstracted, this is just another way of defining Cyber Resilience.

The introduction of *swarm intelligence* into the cyber security field, is a first example of the integration of artificial intelligence techniques in the field of adaptive investigation of the evolutionary behavior of a complex system. In this context, a viable strategy is to use a multi-level agent-based approach, designed to quickly and autonomously adapt to the management of anomalies that are detected, exploiting the semi-rationalization and self-learning characteristics of the agents, settled in a hierarchical arrangement, to interpret and correlate the events on a logic basis, in order to improve communication, interaction and intervention between the human operator and the system. The purpose of the hierarchical arrangement is to provide to humans a single point of influence that allows someone to enable multiple points of effect with a simple action [4].

a. A multi-layer swarm intelligence model

Starting from the last considerations, a well-conceived model is theoretically able to provide an immediate improvement in terms of system capacity in the operations of: detection, risk isolation, situational awareness and response. Fig. 3 shows an example of implementation of a multi-layer swarm intelligence-based analysis model, inspired by the hierarchical structure used by ants. This is a high-level scheme, but it provides a first idea of how to build such platform. At the lowest level of the hierarchy we find the *workers*, i.e. the systems for processing and collecting massive data, including log analyzers, IDS systems, cyber probes, automatic scripts that process or supply data, and so on. These *workers* must have the following characteristics: they must perform only simple operations, they must be able to communicate directly only with the upper level agents, they must be authenticated and they must be present in all the parts of the system. The communication between joint *workers* must be possible only in an implicit way, due to the detection of variations and anomalies that emerge from the observation of the surrounding environment, in full respect of the rules of stigmergy.

The intermediate layer must be careful to scrape the data collected by *workers,* using intelligent data analysis and correlation engines. This level has to take a first series of choices, which can be summarized as follows: generation of alarms to be passed to the higher level for further evaluation, management of direct interventions to block in real time the attacks in progress, and data filtering in order to discard superfluous notifications. At this level we can find the mid-level SIEMs *(male ants)*, which perform the processing and correlation operations, and the IPS and/or EDR systems *(soldier ants)*, which are concerned to intervene promptly on a threat. Theoretically, to make the analysis and correlation activity carried out at this level really efficient, all medium-level devices should be equipped with a self-learning engine.

At the top of the hierarchy we find the high-level SIEM *(queen ant)*, equipped with an advanced data analysis and correlation engine, entirely based on an artificial intelligence brain, able to collect the alarms coming from the various medium-level SIEMs and to extrapolate from them clear, precise and geo-referenced information to be passed to the human operator. The latter will have the responsibility to perform the last level of information filtering that will result in the application of a high-profile intervention process aimed at securing the infrastructure and therefore people safety. Finally it is good to note that not data but information is passed on to the human operator and it is an essential step in order to determine the right behaviour of the model.

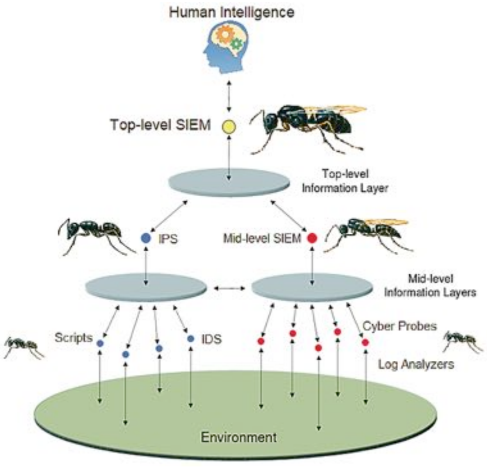


Fig. 3 *Theoretical model of a cyber security framework that makes use of multi-layer swarm intelligence in order to improve the detection, the response, the risk isolation and the situational awareness capabilities of the whole system, inspired by the hierarchical structure of ants.*

Conclusions

The final aim of building and adopting a cyber security framework dedicated to the protection of complex, complicated and critical systems is to save people's lives. The impact of a cyber attack on a critical system can be literally catastrophic, most often completely inadmissible, so it is important to invest in cyber security, in order to search for increasingly efficient strategies that could allow companies to identify and assess threats into a real time manner. Although there is no a definitive solution to all the cyber threats that may jeopardize the natural functioning of these systems, the main goal is to reduce the level of uncertainty linked to the manifestation of a freak as much as possible, by automating properly detection and correlation operations. In this way it would be possible to bring a simple and immediate result to the attention of the human operator. Formally, the introduction of artificial intelligence techniques in cyber security analysis strategies aims at summarizing at most the alert information received from the various devices that make up the system in order to enable the human operator to intervene promptly in safeguarding both people safety and system security.

Abbreviations

- EDR - Endpoint Detection and Response
- IDS - Intrusion Detection System
- IPS - Intrusion Prevention System
- SIEM - Security Information and Event Management

References

[1] Delain, O., Ruhlmann, O., Vautier, E., Johnson, C., Shreeve, M., Sirko, P., Prozserin, V. (2016). Cyber-security application for SESAR OFA 05.01.01-Final Report. OFA 05.01.01-D3.

[2] Gandhi, Gagan. (2014). Complexity theory in Cyber Security. University of Warwick.

[3] Holland, J. H. (1995). Hidden order: How adaptation builds complexity. Helix Books.

[4] J. N. Haack, G. A. Fink, W. M. Maiden, A. D. McKinnon, S. J. Templeton and E. W. Fulp, Ant-Based Cyber Security, 2011 Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, 2011, pp. 918-926.

[5] Oltsik, J., Poller, J. (2017). Automation and Analytics versus the Chaos of Cybersecurity Operations. ESG Research Insights Paper.

[6] S. A. McLeod (2008). Reductionism and Holism. ■

[1] This work was supported by the research activity carried out by Thales Italy on the SESAR2020 project. In particular, SESAR2020 is a research program made up by many projects which aims to design the next wave of the European Air Traffic Management innovation systems. Thales Italy is involved in the development of a couple of these projects, one of which is enterely dedicated to the cyber security.

Data, consumers and trust: the quiet crisis

Building trust-based relationships with clients has always been important for successful business practice. As the global data pool grows and consumer fears over personal privacy increase, it may become make-or-break.

Author: Olivia Green

In the last two years, we have created 90% of the total data in the world today. In a day, we spit out an average of 2.5 quintillion bytes – and counting. From smart watches that monitor our heart rates to chat-bot therapists who manage our anxiety, nearly every aspect of our lives can be digitized. This undoubtedly provides us with immense benefits – increased speed, convenience and personalisation to name a few. Yet it also gives rise to a challenge: how do we protect our right to privacy?

Anxieties over internet privacy are nothing new. As the data pool continues to expand however, they have been picking up steam. Hacks and other tech-related scare stories are now a daily occurrence on our newsfeeds – and they are increasingly hitting closer to home. Back in May 2017, the credit card details and passwords of nearly 700,000 UK citizens were compromised when Equifax fell victim to a hack. Even our private conversations don't feel safe, as it emerged that Google's new Home Mini had been accidentally recording its users without their knowledge.

BIO

Olivia Green is an Innovation Consultant and member of Sopra Steria's Horizon Scanning Team, working to identify social and technological trends that are shaping business and society today. She has a particular interest in data and ethics, and has written previously on subjects including GDPR, blockchain and encryption. She holds an MA in Classics from the University of Edinburgh.

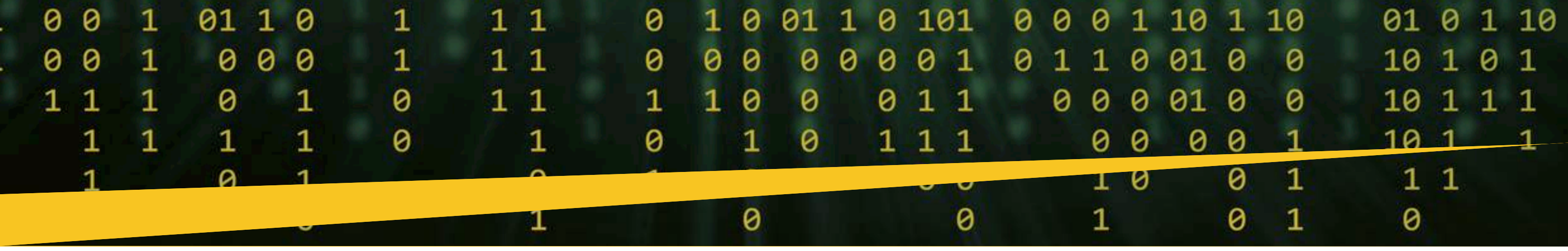
Corporations themselves are also a target of consumer fear, and they are beginning to pay the price. According to recent research, US organisations alone lost $756 billion last year to lack of trust and poor personalisation, as consumers sought out alternatives. UK consumers share similar anxieties; nearly 80% of cite lack of confidence in the way that companies to handle their information as an extreme source of concern, while just under half now view data sharing as a "necessary evil" – something they will do reluctantly if they deem the reward high enough.

These findings aren't an anomaly. Statistics gathered last year by the ICO show that only 22% of UK consumers trust internet brands with their personal data; more shockingly, they highlight that while over 50% of consumers trust High Street banks, only 36% have confidence in Governmental bodies to manage their data properly.

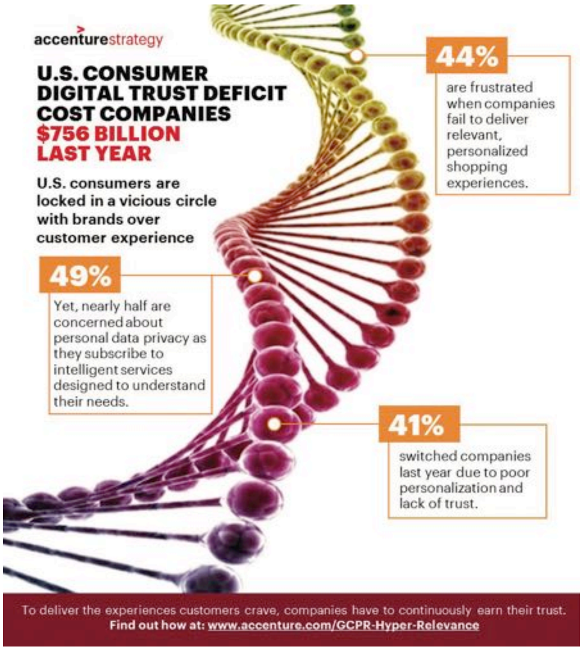
The price of complacency

So far, companies have largely managed to side-step the more serious consequences for consumer mistrust and data mismanagement. Not all have been lucky though. The notorious Ashley Madison hack in 2015 is a prime example of just how damaging loss of trust can be. The website, which provided an online platform enabling married people to conduct affairs, fell victim to hackers who published a digital "name and shame" list of its clients. For a business whose model was so dependent on trust and confidentiality, this proved disastrous. Despite the organisation's insistent claims otherwise, analysis by SimilarWeb revealed that monthly site traffic had plunged since the attack, dropping by nearly 140 million a mere four months after the attack.

For some, the fallout is less dramatic – but still worrying. Take Uber's breach for example, which dragged its already battered corporate reputation through the mud once again after it was revealed that the ride-sharing company had tried to cover up a 2016 data hack affecting 57 million customers. The immediate furore that followed this has raised some immediate problems for the firm, including the threat of prosecution and impending investigations by multiple countries worldwide. Even more problematic for Uber are the wider-ranging consequences of this cover up.



In combination with their potential loss of the London market and recent workplace scandals, this disastrous year has materialised into real financial impact; at the close of this quarter, Uber logged record losses of $1.5 billion, a $400 million increase on previous quarter and a far cry from their triumphant predictions of growth at the beginning of 2017. In a particularly telling sign, Uber's investors also appear to be hedging their bets. Fidelity, who already have a significant stake in Uber, announced recently that they had participated in a funding round for Uber's closest competitor, Lyft, pushing the latter's valuation up to $11.5 billion.



accenturestrategy

U.S. CONSUMER DIGITAL TRUST DEFICIT COST COMPANIES $756 BILLION LAST YEAR

U.S. consumers are locked in a vicious circle with brands over customer experience

44% are frustrated when companies fail to deliver relevant, personalized shopping experiences.

49% Yet, nearly half are concerned about personal data privacy as they subscribe to intelligent services designed to understand their needs.

41% switched companies last year due to poor personalization and lack of trust.

To deliver the experiences customers crave, companies have to continuously earn their trust.
Find out how at: www.accenture.com/GCPR-Hyper-Relevance

©Accenture

Unlike Ashley Madison, Uber's problems arose not so much from the hack itself, but from their attempt to cover it up. But despite the evident lesson here, this is a scenario we could see again. Over 2/3 of UK boards currently have no training to deal with a cyber-incident and estimates suggest that only 20% of companies have appropriate response plans in place. For Uber, the ultimate consequences of its misconduct remain to be seen; for the moment, they are protected by their largely unique offering, which gives consumers limited alternatives. Should it happen to a business without Uber's dominance, it could prove fatal.

Monetising trust

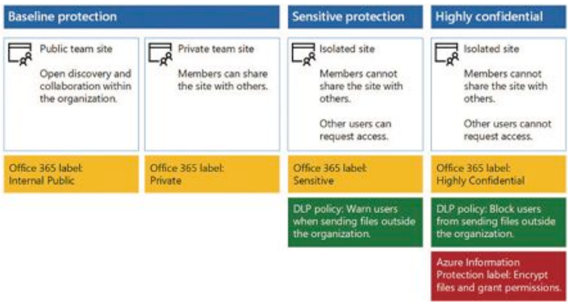
How can organisations move forward from here? In the current climate, it is unlikely that consumers will ever wholly withhold their data, as they place value on the services that giving away that data provide – as much has been shown by the fact that risky "data trade-offs" like Uber manage to survive.

However, as awareness of the risks and the stakes of losing data to a hacker increase, they are looking increasingly selective about who they choose to share their information with. As more and more information shifts from physical to digital, businesses must be prepared for change. We may be heading towards a future where access to data is no longer a handout but a privilege, hard won by effective risk management and transparent, secure systems that hand back sovereignty to the customer. To retain this privilege, businesses – especially those in crowded markets- should make effective data strategies an utmost priority.

Power to the people

So what makes an effective data strategy? For businesses, the answer to this question has, in part, been dictated by the introduction of GDPR in May; but while some businesses have only grudgingly fallen into line with the dictums of transparency and privacy, opportunities exist for those who embrace the new legislation.

Microsoft is example of one such company. In the weeks following GDPR's introduction, it has made much of its new approach to user privacy and data, extending GDPR style privileges to its entire global customer pool (not just those based in Europe), and creating a new, user-friendly data management platform, which empowers individual users to view, maintain and delete data which Microsoft hold on them. Most importantly of all, they have provided clear, detailed information detailing why it benefits consumers to share their data with Microsoft. At its essence, their new approach can be reduced to three key components: respect, access and utility.



Baseline protection		Sensitive protection	Highly confidential
Public team site Open discovery and collaboration within the organization.	Private team site Members can share the site with others.	Isolated site Members cannot share the site with others. Other users can request access.	Isolated site Members cannot share the site with others. Other users cannot request access.
Office 365 label: Internal Public	Office 365 label: Private	Office 365 label: Sensitive	Office 365 label: Highly Confidential
		DLP policy: Warn users when sending files outside the organization.	DLP policy: Block users from sending files outside the organization.
			Azure Information Protection label: Encrypt files and grant permissions.

©Microsoft

This is no simple exercise in corporate vanity. Microsoft's approach has won it favourable comparisons with other big corporates such as Facebook and Google, who remain technically compliant but have tried to manoeuvre around "the spirit" of the legislation – and have consequently faced a significant backlash from clients. It also positions Microsoft as the antithesis of the "evil" corporate enterprise that has now so often come to define big tech – something that will only serve it well in the future.

No company – even those as seemingly untouchable as Google or Uber – can afford to ignore this quiet crisis of trust. In our future digital economy, it is data that will ultimately decide who wins and who loses. It is the lifeblood of capabilities like AI and predictive analytics, and is essential for providing the personalised services such as smart home devices that are becoming increasingly inseparable from modern life. While some businesses may be shielded for the time being by the uniqueness or the scarcity of the service they provide, even they can't afford to breathe easy. As the surging interest in Lyft is demonstrating, rivals are never far behind. ■

Protecting Your Digital Assets Against Cyber Attacks. Cyber Criminals Are Probably Winning. Here is why.

You have been hacked! Those are four words that no organisation wants to hear - ever. The reality is that all organisations are vulnerable to cyber criminals activities.

According to a recent article by Kelly Sheridan (Dark Reading), the Cybercrime Economy Generates $1.5 Trillion a Year!

Author: Marco Essomba

That's a mind blowing figure. In this article, I share some thoughts as to why the current mechanisms of fighting back against cyber attacks are not working. Read on.

BIO

Marco Essomba is a Certified Application Delivery Networking and Cyber Security Expert with an industry leading reputation. He is the founder and CTO of iCyber-Security Group, a leading edge UK based cyber security firm providing complete and cost effective digital protection solutions to SME's. iCyber-Security's cyber defence platform (iCyber-Shield) gives total visibility & control over your entire security infrastructure. The product is listed on the London Digital Security Centre MarketPlace.

Let's connect on Twitter:
33K+ followers –> @marcoessomba
Let's connect on LinkedIn: 11K+ followers:
https://uk.linkedin.com/in/marcoessomba

Cybercrime Pays

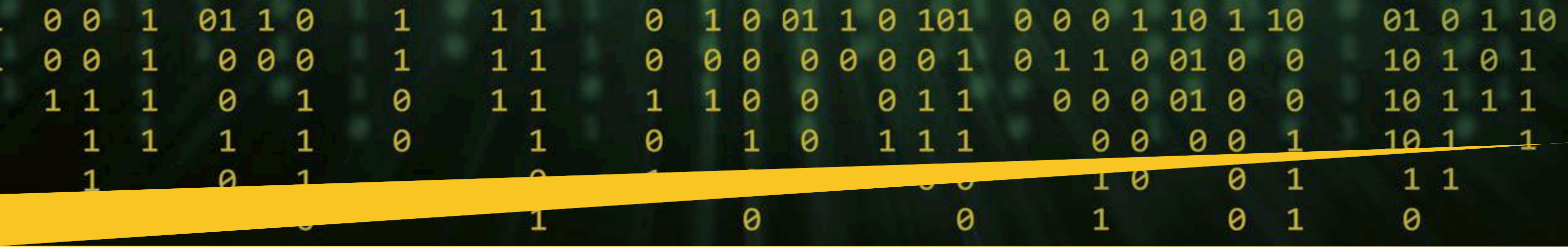
There are many reasons why cyber criminals appear to be winning the fight and reaping the rewards. For one, it is clear that cybercrime pays and most of those criminal organisations now run like legitimate businesses with organised operations, strategies, support, and profits reinvested into research and development efforts.

Those criminal organisations are not much different to security software vendors that are continuously looking for issues and provide updates to patch vulnerabilities and security flaws. It's an always on race.

Lack Of A Fully Integrated Security Ecosystem

Cybersecurity Ventures listed 500 of the world's hottest and most innovative cybersecurity companies to watch in 2017. From Adaptive Security Platforms, Email Security products, to Anti-Virus & Malware Protection, the list is huge. Which one should you use and for what purpose? Will your chosen product integrate well with other security vendors? How do those products compare? There are a lot of considerations that each organisation have to take into account. From the total cost of ownership of the product, ease of use, quality of service, support, etc. In any case, 500 security vendors is a huge menu to select from.

Network & Security Managers have the challenging task of assessing multiple vendors and selecting the product and services that match their organisation's needs. Not an easy task in a very crowded



and noisy cyber security market place. Security analysts have been predicting for a while that the entire cyber security industry is ripe for consolidation. The same thing happened in other sectors like manufacturing, systems management, enterprise applications, and telecommunications. So it makes sense that the cyber security industry will go through the same process.

More Integration, More Consolidation, Less Security Vendors

What is needed is for more security vendors to work together for better integrated solutions and services in order to fight back cyber attacks and cyber crime more effectively. The time for single point solutions is coming to an end. Cyber criminals are coordinating, sharing tools, and intelligence to run effective campaigns and are increasingly reaping huge rewards. This is validated by the relentless and growing number of successful cyber attacks reported in the media on a regular basis.

Humans & Machines Working Together As One

Fundamentally software will continue to have vulnerabilities that can be exploited by malicious attackers for their own gains. As software developers get more adept at secure coding, it is expected that vulnerabilities will steadily diminish but cannot be avoided altogether. Machines are very good at boring and repetitive tasks but lack context and insights. Humans are very good at contextualising and finding solutions in creative ways but lack the repetitive stamina to conduct boring tasks consistently. As machines carry more and more automated security analysis to look for vulnerabilities in various systems, both humans and machines must work together.

Fully Integrated & Coordinated Cyber Defence Infrastructure

Organisations will need to find better ways to integrate their entire cyber security infrastructure and ecosystem in order to respond better and faster to cyber attacks. Like criminal organisations, companies that are serious about cyber security will have to use a defence-in-depth strategies that include a fully integrated security infrastructure that is working as one effective defence system. They should combine traditional network defence mechanisms such as firewalls, intrusion detection systems, endpoint protection, web application firewalls, etc. with external threat intelligence methods, and adaptive threats response, in order to stay one step ahead of cyber criminals.

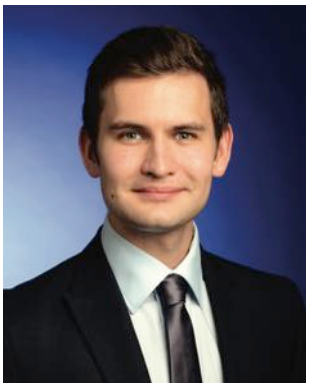
> *Much of the money is reinvested in new criminal ventures. Criminals put about 20% of their revenues into additional crime, indicating up to $300B is used to drive illegal activity.*
>
> *~ Kelly Sheridan, Dark Reading*

Conclusion

The cyber security industry is ripe for consolidation. Too many security vendors. Too many products. What is required is a fully integrated approach to cyber security, where humans and machines work as one, in an self-automated and coordinated manner in order to fight back effectively against the relentless and ever growing cyber threats.

At iCyber-Security, we have developed the iCyber-Shield Enterprise Cyber Defence Platform that allows you to manage, automate, respond, and orchestrate your entire cyber security infrastructure from a single command and control interface, ensuring that ALL your business critical digital assets are secure and always available - 24/7! ■

Poker and Security



Author: Leron Zinatullin

Good poker players are known to perform well under pressure. They play their cards based on rigorous probability analysis and impact assessment. Sounds very much like the sort of skills a security professional might benefit from when managing information security risks.

What can security professionals learn from a game of cards? It turns out, quite a bit. Skilled poker players are very good at making educated guesses about opponents' cards and predicting their next moves. Security professionals are also required to be on the forefront of emerging threats and discovered vulnerabilities to see what the attackers' next move might be.

At the beginning of a traditional Texas hold'em poker match, players are only dealt two cards (a *hand*). Based on this limited information, they have to try to evaluate the odds of winning and act accordingly. Players can either decide to stay in the game – in this case they have to pay a fee which contributes to the overall pot – or give up *(fold)*. Security professionals also usually make decisions under a high degree of uncertainty. There are many ways they can treat risk: they can mitigate it by implementing necessary controls, avoid, transfer or accept it. Costs of such decisions vary as well.

BIO

Leron Zinatullin is an experienced risk consultant, specialising in cyber security strategy, management and delivery. He has led large-scale, global, high-value security transformation projects with a view to improving cost performance and supporting business strategy. He has extensive knowledge and practical experience in solving information security, privacy and architectural issues across multiple industry sectors. Leron Zinatullin is the author of The Psychology of Information Security.

Website: zinatullin.com / Twitter: @le_rond

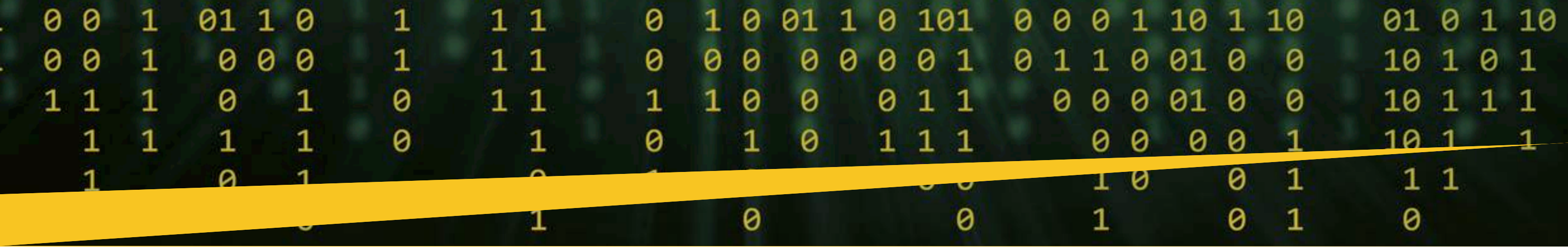
Not all cards, however, are worth playing. Similarly, not all security countermeasures should be implemented. Sometimes it is more effective to fold your cards and accept the risk rather than pay for an expensive control. When the odds are right a security professional can start a project to implement a security change to increase the security posture of a company.

When the game progresses and the first round of betting is over, the players are presented with a new piece of information. The poker term *flop* is used for the three additional cards that the dealer places on the table. These cards can be used to create a winning combination with each player's hand. When the cards are revealed, the player has the opportunity to re-assess the situation and make a decision. This is exactly the way in which the changing market conditions or business requirements provide an instant to re-evaluate the business case for implementing a security countermeasure.

There is nothing wrong with terminating a security project. If a poker player had a strong hand in the beginning, but the flop shows that there is no point in continuing, it means that conditions have changed. Maybe engaging key stakeholders revealed that a certain risk is not that critical and the implementation costs might be too high. Feel free to pass. It is much better to cancel a security project rather than end up with a solution that is ineffective and costly.

However, if poker players are sure that they are right, they have to be ready to defend their hand. In terms of security, it might mean convincing the board of the importance of the countermeasure based on the rigorous cost-benefit analysis. Security professionals can still lose the game and the company might get breached, but at least they did everything in their power to proactively mitigate that.

It doesn't matter if poker players win or lose a particular hand as long as they make sound decisions that bring desired long-term results. Even the best poker player can't win every hand. Similarly, security professionals can't mitigate every security risk and implement all the possible countermeasures. To stay in the game, it is important to develop and follow a security strategy that will help to protect against ever-evolving threats in a cost-effective way. ■



The cyber security awards enter their fourth year in 2018

winner
Cyber Security Awards

Founded in 2015 to reward innovation and excellence in cyber security, the awards have a strong people focus. There are awards for CISO of the year and personality of the year, which celebrate some of the most successful people in the industry. But there are also awards for the best newcomer. Other categories include woman of the year. All awards, highlighting the achievements of some fantastic cyber security professionals. The awards are totally independent, without affiliation to any publication or organisation. It has been this independence, along with the well regarded judging panel, that has led to the awards being recognised as one of the most desired accolades in the industry.

Previous CISO of the year winners include Troels Oerting and Gilbert Verdian. Troels has recently left his role at Barclays, for which he won his award and is now Head of Global Centre for Cybersecurity at the World Economic Forum. Gilbert won for his outstanding efforts at Vocalink in 2017. He has since undertaken roles with the Federal Reserve System and the European Commission. Our first winner, Bryan Littlefair is now one of our judges!

The Woman of the Year category is often a highly contested category. With the goal of celebrating and promoting diversity in cyber, there are a high number of entrants. Vicki Gavin was the first recipient and after a successful time at The Economist, she is now the Data Protection Officer and Head of Information Security for The Northview Group. This year, there is an outstanding shortlist. The shortlist includes women from Deloitte and KPMG who have been instrumental in increasing the diversity in the cyber teams of their organisations and beyond. Emily Biggs at Digital Shadows has made the shortlist for her incredible achievements as part of the organisation. Also included is Mary-Jo de Leeuw. Mary-Jo has been training young people on cyber security and has also managed to have a connected doll banned from stores, after she was able to programme it to talk like a terrorist.

As well as individuals, there are also awards for products and teams. Previous winners of product awards includeYoti, the digital identity app which is experiencing huge success. Nuix Investigation and Response and DNS Shield from Neustar are also previous winners.

A key category this year has been the Cyber Awareness category. This category has grown in size over the past four years, highlighting one of the many changes in the industry. Awareness is now key to many organisations as they realise that breaches often come from human error and that vulnerabilities can be reduced with better training. Amongst the 10 finalists this year are Hacker Girl, a free online cartoon series which has been used to educate individuals about online risk. TalkTalk may not be a name you expect to see shortlisted for a Cyber Security Award but their awareness plan truly impressed the judges this year. Utilising a number of different methods, they have implemented a comprehensive plan, with strong evidence of success and improvements in their key metrics.

Winning a Cyber Security Award can have a hugely positive impact on an organisation. Companies may see an increase in sales, as customers have extra faith in a product that has been independently judged. Organisations that win awards from their security may see extra confidence from their customers. Previous winners of team awards include Arcadia, Vocalink and Camelot. For individuals, the benefits can be significant. CISO's can expect to see a boost in morale from their teams, as well as finding it easier to attract and retain talented individuals to their teams. Those in other categories such as Newcomer or Penetration Tester may find an increase in the amount of job offers they receive! Or they may find a promotion or pay increase is on the card. Being an award winning penetration tester can help their employer win more business, making them a more valuable employee.

If you are considering entering the 2019 awards, the judges have provided some tips on what they look for.

Innovation - The Cyber Security Awards celebrate innovation, in products, strategy and delivery. Every category is looking for the person, team or company who has something fresh to offer.

Passion - Our judges want to see individuals who love the industry and deserve to be celebrated. Getting across your passion for cyber, will see you take that top spot!

Results - A person, team or product that really delivers is key. Have you got board-level engagement or great sales results? We want to know!

Follow the rules - Keep to the word limit, make it easy to read, with no spelling mistakes. We get hundreds of applications, so making it easy for the judges to tell what you are about, really goes a long way.

(Continues on page 23)

How to Avoid Ransomware Jail

It's 1983, and Ronald Reagan is sitting down to watch the hit film *War Games*. Five days later, the president asked his secretaries of state, "Could a scenario like war games ever happen?" One week later, General Vessey returned with the answer: "Mr. President, it is a lot worse than you think."

Author: Darren Swift

Was this the first time that cyber security and privacy had surfaced in computer systems? Categorically, no. *Security and Privacy in Computer systems 1967* by Willis Ware was the first paper on the topic — written in 1967. So, since the beginning of networked computing, cyber security, and privacy have been a factor. So, why is it suddenly a huge industry buzzword?

My thoughts on this are twofold:

1 Across governments, the use and ideas of cyber warfare were dismissed, ignored, or forgotten. But in 2007, the Aurora test categorically proved that cyber attackers could inflict physical damage using computer tools. This was a pivotal moment, as critical infrastructure was at risk.

2 Cybercrime then shifted to the public sphere with cyber groups lining their sights on non-government attacks, such as online fraud, ransomware, malware, and phishing.

The role that security and privacy now play in IT and our personal lives is huge. Strong security practices have gone from a nice interest to an expected standard.

BIO

Darren has over 10 years experience in virtualization, cloud, data protection and automation technologies with a focus in recent years on security in particular ransomware. He specializes in data protection and is self-taught in the realms of cyber security with a focus on ransomware. Self confessed car enthusiast, occasional blogger, snowboarding nut and Rubrik techie.

The Ransomware Problem

Ransomware has dominated headlines over the last few years as businesses were, and still are, targeted. 2017 alone has seen some huge headline attacks – #wannacry #badrabbit #nonpetya – all targeting businesses to encrypt their data and charge ransom. To give you an idea of ransomware's recent success:

- Q1 2016: $209 million in revenue with 2016 totalling $1 Billion
- 56,000 infections per month
- 101 known ransomware families
- Delivery via a range of mechanisms from exploit kits, email, and website links

What many are not aware of is the ecosystem that underpins these ransomware families. The *Cerber* ransomware family, for instance, accounted for 70% of all attacks this year up until #wannacry. This marks the increasing accessibility of "Ransomware-as-a-Service" or RaaS, which is now available to an audience beyond cybercriminal groups.

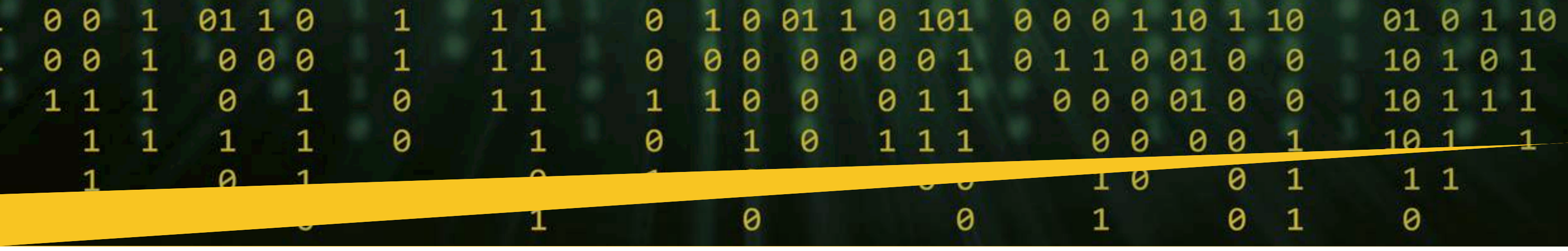
So how does RaaS work? It's the simple franchise-like deployment model. Instead of writing their own malicious code, aspiring cybercriminals can now log in to their RaaS portal of choice, configure their deployment, and instantly distribute the malware to unwitting victims.

Ransomware Sophistication

Early forms of ransomware were not overly sophisticated. But the Cerber family exhibited an unprecedented amount of detail and sophistication.

Some features of Cerber:

- An encrypted JSON file gives the user the ability to change settings (such



as target certain file types), avoid certain language packs or IP ranges, or perform environment checks (looks for AV/VM).

- Modern ransomware looks for almost all file types, including VMware, databases, java-script, and email. It creates multiple Mutex's, gains persistency in Windows, and has fault or watcher processes so that it can be re-spawned.
- If Cerber detects it's being hunted, it will shut down and not run. UAC mode is completely bypassed
- Cerber can encrypt without having any internet connectivity; it has the encryption keys in the payload (RSA-2048)
- Sends statistics via UDP home. Essentially, it will upload statistics of what it discovered in your environment if possible
- Encrypts your data with a high degree of entropy

What Can We Do?

Over the years, I have been speaking about ransomware. By hearing people's ideas and advice across the globe, I've created some basic tips that can help protect against ransomware:

Entry Points (Web, devices, USB and email)

- Use standard practices of scan emails and block USB ports
- Do not enable web access on VMs
- Patch, patch and patch again – just look at the #wannacry virus
- Isolate / different networks for your personal devices

Users and Access

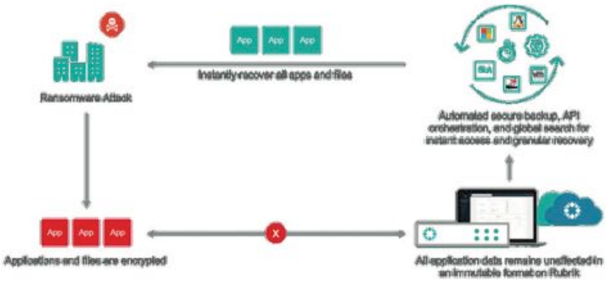
- Train users, both end users and IT users. This is critical in identifying and responding to ransomware.
- Set software restrictions – remove the ability for users to run .exe. While this is radical, if users cannot run a payload, then ransomware cannot run!
- Least privilege access management. Only provide employees access to data to those who need it.
- Audit file shares
- Updated firewalls \ IPS and policies

The Bottom Line

These are just some practices you can use to help protect your data. The bottom line is that ransomware isn't going away, and most customers I speak to (regardless of how many layers of defence are in their environments) admit it's not if but when ransomware will strike. Any report you read on ransomware will state that "backups are a must."

So, what if you are compromised? Don't panic. Here's what I recommend:

- Respond and isolate the spread
- Test before restoring
- Restore
- Root cause analysis


Ransomware Attack
App
App
App
Instantly recover all apps and files
Automated secure backup, API orchestration, and global search for instant access and granular recovery
App
App
App
x
Applications and files are encrypted
All application data remains unaffected in an immutable format on Rubrik

The key here is your response time and getting the affected data back online in the shortest time possible.

So how would you do this ? … one solution is from Rubrik which delivers a highly-automated backup with near-instant RTO. But, most importantly, all the backups are immutable, so they can only be *read* not *over written*. Protecting your valuable data with a highly-automated backup platform is key in having the assurance that, should ransomware infect your environment, you can recover quickly.

Conclusion

Ransomware is not going away anytime soon. So, it's imperative that businesses across industries adopt a data management strategy of multi-layered security, easy automation, and quick recovery. Want to learn more? For further information visit www.rubrikdr.co.uk or call Core DataCloud on 0207 157 9845. ■

The cyber security awards enter their fourth year in 2018

(Follows from page 21)

The following categories will be open for applications soon.

- CISO of the year
- Newcomer of the year
- Personality of the year
- Woman of the year
- Penetration tester of the year
- Consulting practice of the year
- Banking or financial services team of the year
- Industry team of the year
- Not for profit team of the year
- Best security company of the year
- Cyber security start up of the year
- Innovative product of the year
- Innovative product – threat detection
- Innovative product – cloud based
- Cyber awareness plan of the year

http://cybersecurityawards.com

Money talks, for the first time in 5 years

In the 2018 BeecherMadden salary survey, obtaining a pay increase was the top reason for moving jobs within cyber security. For the past 5 years, career progression has been listed as the top reason for moving roles.

Author: Karla Reffold

Cyber security has been growing rapidly as an industry, and in the consciousness of the organisation. It is inevitable that people in the industry saw this as a good opportunity to get ahead, especially after so many years of being under-resourced and under-financed. During this time, we saw salaries increase year on year, as companies fought to attract talent to their teams and organisations invested heavily in building their security functions. We also saw individuals being promoted ahead of their experience level; there were many who became CISO's with just a few years security or risk experience. It is highly possible that as the industry reaches a level of maturity, getting ahead is no longer as important as being paid an attractive wage. An increase in inflation and effective wage stagnation country wide, may also be having an effect on this. With Brexit on the horizon there is slightly less certainty in our economic position & financial position, this may be playing higher on people's minds in general.

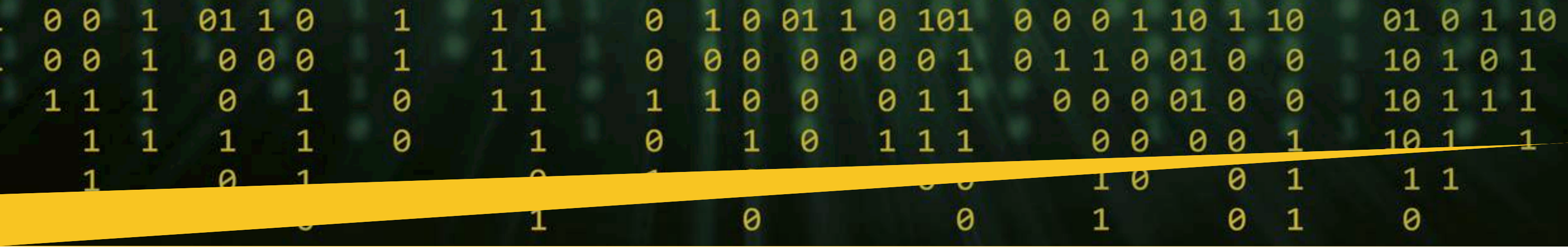
79% of those surveyed by BeecherMaddenexpect to move roles within the next year. This is a scary number for organisations who often expect attrition closer to 20%. Recruiters often target "passive candidates"; those who are not specifically looking for a new role but are open to a move. They have long been considered the best candidates to target, however it is considered "easier" for companies to attract talent by targeting those who are actively engaged in a job search. A better work-life balance also scored highly as a reason for moving roles, followed closely by an increase in flexible working. Many companies have recognised that the market demands some flexibility and offer this in roles that traditionally were more office based. Flexible working and working from home is now a more

Job title	Years of experience	Salary bands
Analyst / Associate	1-3	£28,000-£40,000
Officer / Senior Analyst	3-7	£40,000-£60,000
Manager	7-12	£60,000-£75,000
Senior Manager	7-20	£75,000-£95,000
Head of	3-7	£110,000-£150,000
Director	7-12	£120,000-£170,000
Global Head / CISO	12-20+	£175,000-£450,000

BIO

Karla Reffold is the MD and Founder of BeecherMadden. Karla has over 12 years recruitment experience, building teams in cybersecurity up to C-level. Founded in 2010, BeecherMadden are a leading recruitment company for the cybersecurity industry. Leveraging our long-held relationships, industry knowledge and data driven approach, we help companies and candidates make better hiring decisions.

BeecherMadden are a leading cyber security recruitment company with offices in London, New York, Singapore and Zurich. Established in 2010, we leverage long held relationships, industry knowledge and data driven approach to help companies and candidates make better hiring decisions.



widely offered benefit and candidates are more comfortable asking for this upfront. Over 50% of candidates have flexible working as a current benefit in their role.

Up until 2016, salaries within cyber security had been increasing at a rapid pace, with candidates achieving increases of up to 30% just for moving roles. However, over the past two years, organisations have become wiser to what they are looking for from individuals. Teams are now more mature and hiring the right people, with the right skills, at the right cost has become more important than building a team. Organisations are prepared to wait longer to hire someone, rather than hiring an under-qualified individual. As organisations have built better security leadership capability, they also have knowledgeable individuals in charge of these decisions, as opposed to previous years when they may have been learning as they evolved. We have seen organisations offering much smaller pay increases, and at times no pay increase, as they refuse to fight against market forces and look to achieve fair wage growth across the organisation.

Some roles have bucked that trend, generally roles that are highly specialist. Security architects are now achieving salaries of up to £120,000. 2 years ago, very few were paid above £90,000 with some organisations paying their security architects as low as £65,000. Roles in incident response have also been in line for large increases. If you consider the maturity of cyber security teams this makes sense. More organisations have built SOC's in-house and require more individuals who are experienced in managing incidents and effectively mitigating risk. As always, individuals who are technically skilled and can communicate these issues to the business, are the most in-demand and the most highly paid.

Job title	Years of experience	Salary bands
SOC Specialist	1-3	£35,000-£55,000
Penetration Tester	2-7	£55,000-£90,000
Penetration Tester CHECK or eqv qualified	4-12	£60,000-£110,000
Data Protection Manager	4-12	£60,000-£120,000
Incident Response	3-7	£65,000 - £90,000
Security Architect	7-12	£80,000-£110,000
eForensic specialist	4-7	£30,000-£65,000
IDAM specialist	4-7	£40,000-£75,000

Unsurprisingly, the other area that has experienced high salary increases, is data protection. With the introduction of GDPR, organisations paid high daily rates to individuals to help them get their processes in place. Many data protection contractors were being paid in excess of £1200 per day. When roles became permanent, organisations have been paying over £100,000 and often closer to £150,000 for individuals with strong experience in data privacy. In turn, the large increases for architects and data protection professionals has spurred an increase in wages for CISO's. While the CISO salary bracket is large, there are more individuals than ever being paid over £300,000 for taking on this role. The most common salary bracket at a CISO level is £150,000 to £180,000 but it is now rare to find true CISO roles paying less than £130,000. Many individuals do not want to take on the huge responsibility for less than they are paying some of their team. They are also very aware of the value of what they protect, as well as the potential outcomes if organisations under invest. Not paying your CISO enough, is a strong signal that investment for necessary security functions will not be forthcoming.

Candidates should:

- **Have realistic expectations.** Make sure that the salary you are looking to achieve is actually likely for the roles you are qualified to do. Having expectations that can not be met, will mean that it takes you far longer to secure a new role.
- **Benchmark their experience.** Talk to your recruiter to understand how your experience and salary compares to others in the market.
- **Consider adding to their skills.** If getting ahead in your career is the motivator, then try and take on additional projects or training that will help you achieve that sooner.

Companies should:

- **Make sure they are paying a fair salary for the role.** Under-paying will mean that you are not able to recruit your role, having the role sit vacant for a long time, and likely cost the organisation more by not recruiting someone.
- **Consider their leadership team.** Having a well respected security leader, can help you attract and retain individuals who will be excited to work for, and learn from, someone recognised by the industry.
- **Consider the requirements of the role.** Making sure that the role contains requirements that are truly necessary will help you get to the best person quicker. Often we see job descriptions that contain requirements not truly relevant and this can be off-putting to candidates who assume that the company does not know what they want.
- **Move quickly.** Taking too long to move through the hiring process guarantees you will lose candidates to competitors who are able to interview and offer candidates sooner. ■

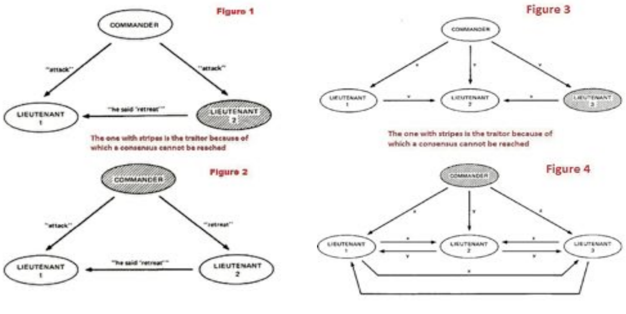
A historian's observations on the worst blockchain problem, the "byzantine fault."

Author: **Laurent Chrzanovski**

One of the worst nightmares for the best blockchains, based on decentralized and distributed systems, is to become vulnerable because of a **"byzantine fault",** i.e. *"a fault presenting different symptoms to different observers"* (Ayala 2016, p. 27)[1].

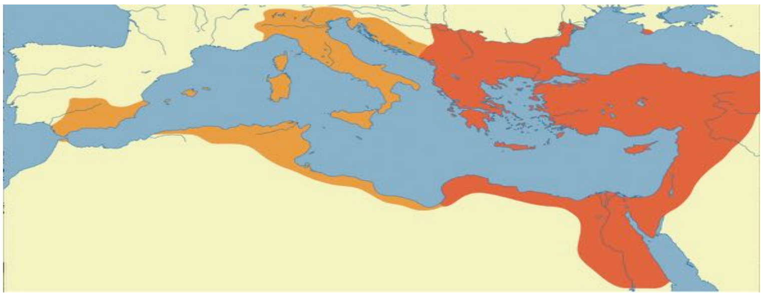
To counter this in fully automated systems, some companies developed a strategy named "Byzantine fault tolerance", i.e. services assuming there are not too many components being in a faulty state. As an example. Ayala quotes *"some aircraft systems, such as the Boeing 777 Aircraft Information Management System and the Boeing 787 flight control systems, use Byzantine fault tolerance".* The problem is nevertheless persistent when humans have a word to say, and may lead to a *"Byzantine failure hack",* meaning that when facing problems, the control center (human or automated) fails to reach an agreement with the components (human or automated) building the system itself, resulting in a dramatic failure of the whole system and creating a door wide open to hackers.

But what is the origin of this expression? It is in fact a shortcut of a longer tile, invented by three top researchers of SRI International. The final result of their study, commanded by the US Army Research Office on ballistic missiles systems, was published in 1982 as *"The Byzantine Generals Problem"*[2], synthetized in the four following schemes:



© Lamport, Shostak, Pease and ACM, 1982

But is it true that historically this was a real problem for Byzantine commanders? Not at all. The authors, probably did not have enough insight of the Byzantine Empire's army. In fact, the empowered generals had full power. The best of them were among the most brilliant the world ever knew, such as Flavios Belisarios (505-565), who alone, doubled the surface of the Empire, taking possession of more than half of the former Roman Empire, thanks to a rock-solid and perfectly commanded army. The Empire, born in 330 as the Eastern Roman Empire, proved a great one, with great generals, at least until 1204.



The Byzantine Empire before (in red) and after (in red and yellow) Belisarios' conquests © Wikipedia

Yet the brilliant IT researchers were not totally wrong on their choice of title. The problem they underlined and alluded to appeared only after 1203, when the Crusaders from acrosl Europe decided not to fight anymore for Jerusalem and to stop at Constantinople.

After the felony and the complete sack of the capital, Constantinople in 1204, itself by those Christians - the famous San Marco bronze horses stolen from the hippodrome of Constantinople were then taken to Venice. – After this point, Byzantium and its Empire never really recovered economically and military, even if its final falletook place 250 years later, in 1453, when Constantinopleewas taken by the Ottomans.

During those last 250 years, Byzantium had the strongest army of all Christianity, but could not go alone to war against its different enemies. Byzantine generals commanded in fact only their troops, the rest being constituted of different Christian groups each led by its own warlord and not a subject of the Byzantine general. This led to many Treasons, misunderstandings, huge mistakes, which further led to many victories but at the cost of a massive lost of men for the Byzantine army and also many defeats which turned to a complete disaster, due to the early hurried attacks or unannounced retreats by those auxiliarys groups.

It is this fact the IT specialists pointed out. The core problem beingdthe very sad lack of cohesion of the main allied commanders, with the byzantine generals, oveg two centuries. For those interested, this phenomenon is masterly depicted by S. Kyriakidis[3], one of the most prominent scholars of this period.

Coming back to the title and therefore the IT problem, we can hence observe the simple lack of an adjective: late. the correct title would have been *The late Byzantine Empire Generals Problem.* ■

[1] Cf. L. Ayala, Cybersecurity Lexicon, New York 2016, p. 27
[2] Leslie Lamport, Robert Shostak, Marshall Pease, The Byzantine Generals Problem, in ACM Transactions on Programming Languages and Systems,Vol.4 , No. 3, July 1982, pp. 382-401.
[3] Savvas Kyriakidis, Warfare in Late Byzantium (1204-1453), Leiden 2001

web for your business
swiss webacademy

together with:

AGORA
poţi să ştii!

iCyber-Security
SAFEGUARDING YOUR DIGITAL WORLD

Present:

CYBERSECURITY ROMANIA CONGRESS
6th Edition

6th Central European Cybersecurity Congress

A Public-Private-User Dialog Platform
September 13-14, 2018, Sibiu, Romania
https://cybersecurity-romania.ro

With the support of: ITU

Under the High Patronage of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

In partnership with:

ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

ROMANIA SRI Patria a priori SERVICIUL ROMAN DE INFORMATII

ROMANIA CENTRUL NAŢIONAL CYBERINT SERVICIUL ROMAN DE INFORMATII

IGPR
POLIŢIA ROMÂNĂ

DIRECŢIA DE COMBATERE A CRIMINALITĂŢII ORGANIZATE I. G. P. R.

CERT.RO

GLOBAL CYBER SECURITY CENTER

Gendarmerie nationale
Une force humaine

RÉGION-IHEDN FRANCHE-COMTÉ

Centre de recherche de l'EOGN

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

POLICE GENÈVE

IATA

FIC 2018

CCI TERRITOIRE DE BELFORT

SIBIU COUNTY COUNCIL

ULBS
Universitatea "Lucian Blaga" din Sibiu

1948
UNIVERSITATEA DIN PETROŞANI

Vallée de l'Energie