ISSN 2738-7097 https://doi.org/10.11610/cybsec02

British Embassy Sofia

# Cybersecurity Newsletters

IICT
Institute of Information and Communication Technologies

## UK-BG Partnership in Cyber Security for SME and Organizations

Newsletter August 2020 Number 2

## Aims and Scope

The present online newsletter is addressing the topic "Risks & Challenges to Data Protection in COVID – 19 era", giving accent to the cyberspace security landscape dynamics during the first wave of the pandemic lockdown. Further details are also given to the expectations of the post-lockdown effects and the plausible & implausible cyber security expectations for the near future in COVID-19 age. Some supplementary explanations of the defined cyber security landscape dynamics are also discussed.

Additional accent is outlined to the future of data protection trends, incorporating the data classification high security added value. The process is considered as the one for data appropriate categorization. This guarantees a more efficient data use and protection across corporate networks. In this context, a layered data classification solution from UK Boldon James company is also provided, being one of a kind world best practice approach. Next, Data Loss Prevention (DLP), encryption and Rights Management are marked as a natural follow-up from the GDPR regulations perspective, accentuating on DeviceLock EndPoint DLP Suite. The solution is allowing comprehensive management of different data states (rest, motion, transit, use) and devices complex architectures in corporate environment.

The current issue is next briefly introducing the reader with some of the leading UK institutions and initiatives in the field of security and in particular – the Defence Science and Technology Laboratory (Dstl), being an executive agency of the Ministry of Defence, UK. The Cyber Systems Programme of UK Dstl is also marked as an integral part of a cross-government transformative programme intended to deliver highly-effective and evolutionary UK cyber capabilities, ensuring a more country-resilience to cyber attacks, exploiting the opportunities of cyberspace.

From Bulgarian side as an initiative is announced the "Secure Digital Future 21", combining both research & educational efforts throughout a proven expert community with valuable partner support from about 50 countries on the five continents around the world.

The Union for Private Economic Enterprise (UPEE) is the SME/ME & micro-nationally recognized employers' association noted in this issue. As one of the leading partners in Bulgaria for policymaking, whilst preserving its political independence. The organization has a sustainable interests & partnerships in the last several years in the area of cybersecurity issues industrial aspects.

In the more applied part of this issue, ten practical recommendations for data & information protection to SMEs/MEs are edged, together with recent cyber vulnerabilities from leading industrial representatives, like: CISCO, Microsoft, Google, WordPress, Facebook, Autodesk & GNU/Linux. Finally, some additional links of cyber related institutions from Bulgaria, UK & internationally are also marked.

Issue Editor: **Assoc. Prof. Zlatogor Minchev**

# Issue Focus: Risks & Challenges to Data Protection in COVID - 19 era

Assoc. Prof. Zlatogor Minchev
CISO at IICT, Issue Editor

In todays' world the technological progress is constantly shaping our reality with new smart solutions and services. This from one hand is moving our society towards a new level of total digitalization, and from another – opens the Pandora's box of unprecedented security risks and challenges. The latter are combining a triplet of: humans, technologies & environment that due to both internal and external issues are getting quite important for the very transformational process of the new digital reality mix of people, machines, biotope & intellect. The transformed social reality of year 2020 dominated by COVID-19 pandemic so far, is for the first time in our new century history, establishing a security landscape that needs to handle the technological, societal & biological aerials uncertain clash dynamics in a rather demanding way.

Therefore, it is quite important to note three main problems that need to be coped proactively by the CISO analytical team:

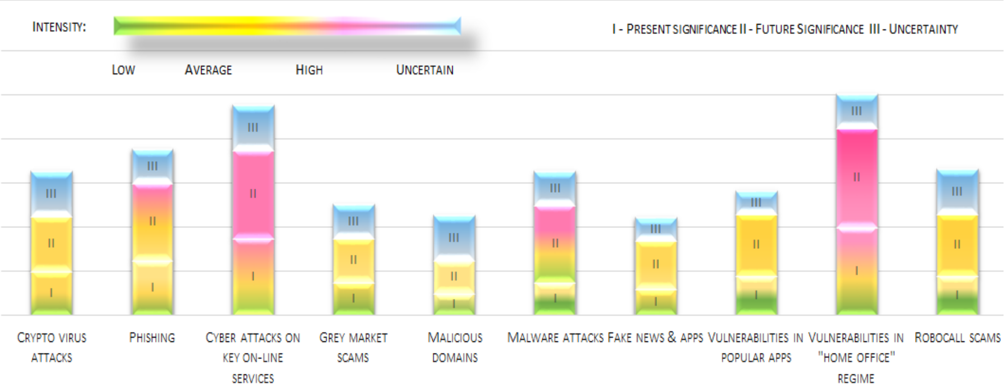
- What have been the challenges, risks & conclusions for the cyberspace security landscape dynamics during the first wave of the pandemic lockdown?
- What are the post-lockdown effects on the cyber security landscape?
- What will be the plausible & implausible cyber security expectations for the near future in COVID-19 age?

Being however not just informative but oriented towards the business data & information protection, further some useful practical recommendations are also presented.

## Cyberspace security landscape dynamics in the first wave of COVID-19

The results from the first wave of COVID-19 with proactive prognosis for year 2020 could be summarized around "ten most current socio-technological risks and threats", analysed at the Institute of Information and Communication Technologies of Bulgarian Academy of Sciences.

Priorities are given to key online services and vulnerabilities in the "Home Office" working organization. Other important ones: phishing threats and malware attacks. Growth in significance, but to a smaller extent, is also expected in terms of crypto-virus attacks, vulnerabilities in popular applications, robocall scams, fake applications and news, grey-market scams and malicious domains.



## COVID-19 post-lockdown effects on the cyber security landscape

Aside from the proactive nature of the preliminary analytical findings of the COVID-19 first wave, some additional aggregations have been recently observed and deserve to be marked here after:

- AI Enhanced Hybrid Threats – hybrid by means of human-machine intelligent interaction, inspired for fake news, fake social networks accounts, contacts & spam generating;

- Smart Infrastructure Attacks – mainly related to IoTs and remotely controlled smart home devices, cars, cameras but also within supercomputer facilities.

The inspiration for these attacks could be found in economic benefits searching due to multiple negative trends throughout the world, caused by the economy delay & unemployment growth. Another reason is probably originating from the hacktivism necessity of the younger generation, basically related to the negative social effects and overall political disagreements of the lockdown during COVID-19 first wave.

### Plausible & implausible cyber security expectations for the near future in COVID-19 age

Going beyond the post-lockdown COVID-19 effects is a quite challenging and arguable research field, being dependent on multiple social, biological and technological factors. So, in this sense, a simplification to some plausible and implausible expectations could be further outlined, providing a somewhat aggregated digital reality mix uncertainty handling:

*Plausible:*

- Data Breaching;
- HW & SW Innovations Vulnerabilities;
- Resources & Know-How Compromising.

*Implausible:*

- Cyber Revenges & Terrorism;
- Resources Hidden Exchange;
- Entertainments Related Attacks.

Further supportive understanding of this mixed reality security changes could be outlined due to: future companies market & clients competition growth caused by negative socio-economic environment development trends, users sustainable interest towards innovations from the technological world (including multiple new services, gadgets & apps) & motivation to escape in a parallel & more colourful digital reality that entertains mostly the youngsters, being demotivated from potential future social isolation & overall lifestyle transformation.

## The Future of Data Protection - Best Practices from UK

### The Future of Data Protection – Best Practices from UK

Securing the new digital era is also connected to a new level of data protection – one that assures greater protection for data subjects, stronger regulatory oversight and even larger fines for non-compliance. While data classification offers an increasingly persuasive answer to the questions of unintended data leakage, it doesn’t stop here. Thus, the benefits of effectively categorizing data go far beyond protection.

Data classification is the process of organizing data into appropriate categories for more efficient use and protection of data across corporate networks. In the security context, data is tagged based on its level of sensitivity, making it easier to find, track and secure, according to its sensitivity rank. In this manner, data classification significantly contributes to risk management, regulatory compliance and data security.

For an effective data classification policy development, categories need to be kept simple, so all employees can properly apply them. While these vary according to companies’ necessities, four major categories are usually used when it comes to sensitive data:

- Highly sensitive data: information that, if made public, puts the company in danger of legal action, regulatory noncompliance or financial loss. This refers especially to personally identifiable information, but also company records and other categories of data deemed sensitive depending on the industry;

- Internal sensitive data: information that, if revealed, can pose a risk to company operations. These include sales data, customer information, employee salaries, etc.
- Internal data: information that while not sensitive is not publicly available such as organizational charts, marketing strategies, etc.
- Publicly available data: information that everyone within and outside the organization has access to, for example, product descriptions, company address, etc.

As the objective to categorize all data in a company is a reasonable one, only few companies can allow it. Given the enormous amounts of data organizations nowadays process, it's only natural that tagging every item of data is a cumbersome, time consuming and ultimately expensive endeavour. It is therefore essential that companies build their own data classification categories that include both sensitive data as defined by various regulations that they are obligated to comply with, as well as what can be considered as industry-specific sensitive information.

Making sensitive data easily identifiable to a data processor is essential under new regulations such as the GDPR that require companies not only to be able to find such data and protect it, but also to demonstrate their processing capacity. It is also important for organizations to comply with users' requests to access or erase their personal data within a given time frame. Failures in this task accomplishing could result in heavy fines and a loss of customer trust.

Data classification extends the value and efficacy of your wider data security and governance ecosystem, to mark – adding new levels of intelligence to data loss prevention or data archiving solutions. All of which drives greater levels of return across your data protection investments. Ultimately though, data classification allows data security controls, rules and policies to be more easily and consistently enforced.

## What is Data Classification?

Data classification is fundamental for protecting and managing data, but it can do much more for business securing. The primary reason most organisations look at classifying the data they create and handle is to control access to sensitive information, driven by the need to manage security risk and comply with regulations, such as GDPR. This scope is however too narrow. By focusing solely on these objectives, they're missing an opportunity to embrace data categorization and extract greater business value from all of their data assets.

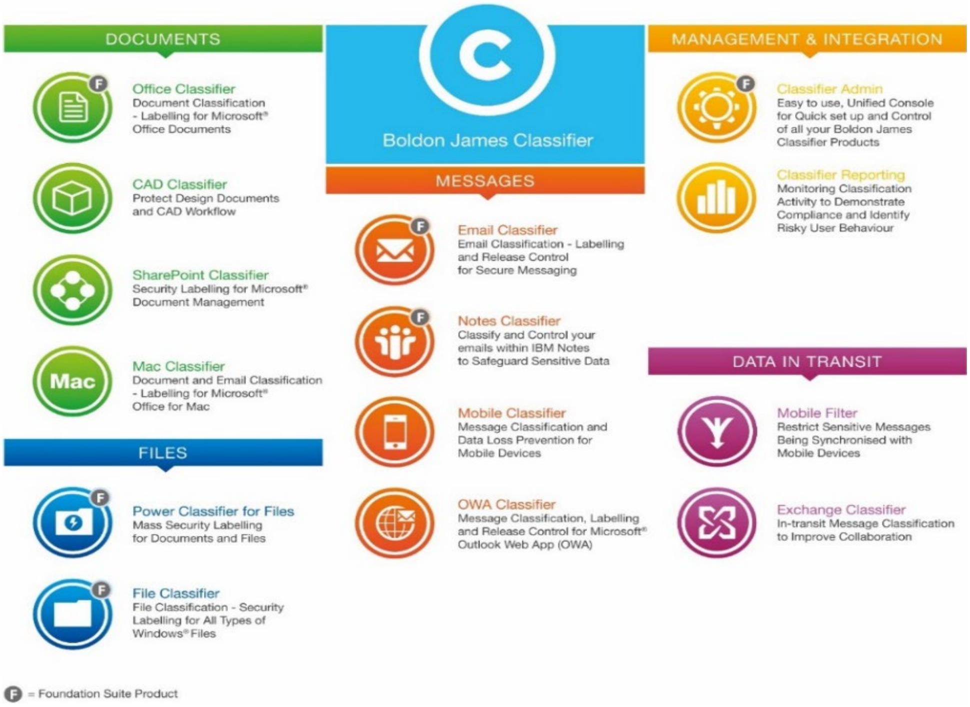
## Data Classification and Regulations

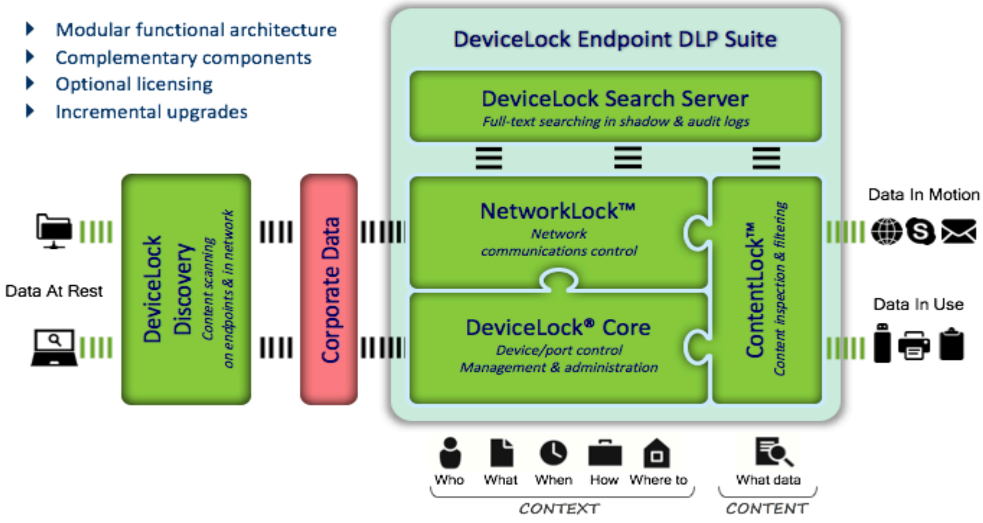
All organizations have to comply with the rules of their industry bodies and the nation-states they operate in. Achieving compliance is complicated. There is a myriad of tools available to support the protection and control of data, ranging from point products to whole integrated suites. All of these consume your budgets for capital and operational expenditure. So, what's the benefit of all that investment? A possible reduction in the size of a fine resulting from a compliance failure is certainly a laudable objective, but there have to be better reasons than that to invest.

There is a growing trend for Data classification customers to ask broader questions around their information. They are taking a wider perspective of the problem, moving from "we have all this data – we need to protect it", to "we have all this data – we want it to work harder for us". To identify additional benefits of controlling data we need to look beyond just compliance and governance and focus on the business – what it does, where it does it and how it does it – to reveal the information assets that underpin all business processes. The tools and approaches used to achieve compliance have a much wider role to play within the enterprise, in helping you to get the maximum value from these information assets.

## Layered Security Approach

Data classification solutions, as UK Boldon James Classifier bridge the gap between the more traditional perimeter IT security solutions (such as firewall protection) and information management solutions. Increasingly, data classification is becoming a best-practice part of a layered security approach, which may include Data Loss Prevention (DLP), encryption and Rights Management. Once data is appropriately classified, security tools such as DeviceLock EndPoint DLP Suite, policy-based e-mail encryption, access control and data governance tools are exponentially more effective, as they can access the information provided by the classification label and metadata that tells them how data should be managed and protected.


DOCUMENTS
Office Classifier
Document Classification - Labelling for Microsoft® Office Documents
CAD Classifier
Protect Design Documents and CAD Workflow
SharePoint Classifier
Security Labelling for Microsoft® Document Management
Mac
Mac Classifier
Document and Email Classification - Labelling for Microsoft® Office for Mac
FILES
Power Classifier for Files
Mass Security Labelling for Documents and Files
File Classifier
File Classification - Security Labelling for All Types of Windows® Files
Boldon James Classifier
MESSAGES
Email Classifier
Email Classification - Labelling and Release Control for Secure Messaging
Notes Classifier
Classify and Control your emails within IBM Notes to Safeguard Sensitive Data
Mobile Classifier
Message Classification and Data Loss Prevention for Mobile Devices
OWA Classifier
Message Classification, Labelling and Release Control for Microsoft® Outlook Web App (OWA)
MANAGEMENT & INTEGRATION
Classifier Admin
Easy to use, Unified Console for Quick set up and Control of all your Boldon James Classifier Products
Classifier Reporting
Monitoring Classification Activity to Demonstrate Compliance and Identify Risky User Behaviour
DATA IN TRANSIT
Mobile Filter
Restrict Sensitive Messages Being Synchronised with Mobile Devices
Exchange Classifier
In-transit Message Classification to Improve Collaboration
F = Foundation Suite Product



Many organizations have invested in security technologies from which they have yet to derive the benefits they had hoped for or, indeed, been promised. A good example is a Data Loss Prevention (DLP) solution. Organizations using DLP solutions commonly experience frustration with poor end-user acceptance, event management overload and a constant need to refine policy and rules. When data is classified by the users that understand its context, through the application of metadata in the message or file, DLP tools can act on this additional contextual information to provide more effective results, with fewer false-positive errors, improved user experience and greater overall risk reduction.

# Cyber Institutions & Initiatives in UK & Bulgaria

## Defence Science and Technology Laboratory

The **Defence Science and Technology Laboratory** (Dstl) is an executive agency of the Ministry of Defence (MOD) of the United Kingdom (UK) running along commercial lines. It is one of the principal government organisations dedicated to science and technology in the defence and security field. Formed in 2001 year, due to split of the Defence Evaluation and Research Agency (DERA). Dstl was initially engaged with science and technology work that is best done within government, while industrial work of DERA was transferred to Qinetiq, a government-owned company that was later floated on the stock exchange. In 2018, Dstl absorbed the Home Office's Centre for Applied Science and Technology (CAST), taking the engagement of applying science and technology to support the Home Office's operations and frontline delivery, provide evidence to support policy, and perform certain regulatory functions. Presently, Dstl is a proven national asset, giving the UK clear advantage across science, technology, cyber and information.

## DSTL Cyber Systems Programme

The **Cyber Systems Programme** of UK Defence Science and Technology Laboratory (DSTL) is an integral part of a cross-government transformative programme intended to deliver highly-effective and evolutionary UK cyber capabilities, ensuring that the UK is more resilient to cyber attacks and can exploit the opportunities of cyberspace.

Specifically, the programme is engaged with:

- contribution to cyber policy by providing S&T advice;
- evaluation of cyber defence products and services from industry in support of acquisition maintains a sovereign cyber vulnerability investigations capability to protect our platforms, systems and infrastructure from cyber attack;
- developing novel sensing and visualisation methods to capture, process and accurately convey information about actual or likely real-world impact of events in cyberspace.

## Secure Digital Future 21 Initiative

**Secure Digital Future 21 initiative** has been established in 2017 with NATO Science for Peace & Security Programme after-action sustainable support for the celebration of the 10 Years' Anniversary of Joint Training Simulation & Analysis Center, Institute of ICT, Bulgarian Academy of Sciences.

The initiative has been established at the rise of the new technological and social revolutionary transformations for combining both – research & educational efforts in a sustainable knowledge capacity throughout a proven expert community with valuable partner support from about 50 countries on the five continents around the world.

The key objective is to create a digital web portal for expert & research thoughts, innovations and concerns exchange, regarding the new cyber-physical transformed ecosystem of living, encompassing: technologies, knowledge, people and self-evolving AI for successful establishment of the future digital society.

In this manner the founders' belief that will be able to better understand the future digital transcendental effects and prepare the society for successfully meeting of the upcoming security landscape tangible & intangible transformations.

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE

The **Union for Private Economic Enterprise** (UPEE) is a nationally recognized employers' association. In its 30-year history, UPEE has established itself as one of the leading partners of the state apparatus in policymaking whilst preserving its political independence. UPEE members are predominantly representatives of the Small, medium, and micro-enterprises. In 2018, UPEE has started an initiative to build a community focused on emerging technologies and cybersecurity thus becoming an important partner of the digital community in Bulgaria. Since then the Union has attracted as members and close collaborators the Bulgarian Cyber Security Association, the Association of the Certified Ethical Hackers, The Bulgarian Drone Community, Bulgarian Cluster for Artificial Intelligence, and many others. As a national employment association, UPEE is part of the policy making process in Bulgaria through its participation in a number of joint activities. Since 2019, UPPE is an active member of the European Cyber Security Organization (ECSO). In 2020, UPEE and ECSO entered into a contractual agreement for common assignment of the "Cybersecurity made in Europe" label. In 2020, UPPE and the Institute for Information and Communication Technologies (IICT) at the Bulgarian Academy of Sciences signed a memorandum of cooperation. The common goal of the two organizations is to facilitate the process of secure digitization of Bulgarian SMEs.

## Ten Practical Recommendations for Data & Information Protection to SMEs/MEs

Achieving successful data & information protection in the new transformed digital reality influenced by COVID-19 pandemic socio-technological challenges & risks is a complex dynamic task that combines both machine & human intelligence. Special accent in this sense could be given to ten selected protection measures marked here after:

- Preliminary Data Classification Systems implementation for achieving suitable digital landscape for further comprehensive (data, people, devices) securing;
- Cloud or standalone regularly updatable antivirus & antimalware protection platforms (including mobile devices) with: good anti-spam & anti-phishing filtering, reliable back-up systems (both on server with RAID storage or wearable protected device) implementation;
- Periodic security administration and update of the base & system software, including suitable patching and sustainable archiving;
- Effective configuration & implementation of Threat Intelligence Systems, Intrusion Detection Systems, Intrusion Prevention Systems, Data Loss Prevention, Password Management & Firewalls;
- Business Continuity Management solutions & Disaster Recovery systems & procedures usage;
- Risk Management Strategies with relevant security policies development & implementation with suitable external access to corporate resources via secured Virtual Private Networks for remote access;
- Regular training with security awareness innovations, cyber hygiene, assuming world proven best practices for data & information secure handling;
- Elevated access, data & information exchange control on: social networks accounts, gaming cloud services & external smart devices with autonomous network connectivity, including unregistered wearable memory storages in the office environment;

- Verification of the technological solutions, services providers reputation & origin;
- Omitting implementation of third-party products, solutions & services, or the ones from the grey market, on important computer configurations, mobile platforms and private networks.

## Some News on Recent Cyber Vulnerabilities

### INTERPOL report shows alarming rate of COVID-19 cyberattacks

An INTERPOL assessment report of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure. With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption. Key findings highlighted by the INTERPOL assessment of the cybercrime landscape in relation to the COVID-19 pandemic include: Online Scams and Phishing, Ransomware and DDoS, Data Harvesting Malware, Malicious Domains, Misinformation. INTERPOL reports…

### Newly discovered vulnerability "BootHole"

A newly discovered vulnerability (CVE-2020-10713) dubbed "BootHole" in the GRUB2 bootloader threatens billions of Linux and Windows devices allowing attackers to interfere with the boot process preceding the OS startup and to potentially get full control of systems. ZDNet reports…

### Cisco Small Business Switches & Products Vulnerabilities

Cisco has highlighted above 60 new vulnerabilities in Cisco Small Business Switches, Webex meeting, cameras and other software solutions. Among them are about 20 severe threats and 2 critical ones – addressing Cisco Enterprise NFV Infrastructure Software & remote code execution, denial of service (DoS), or information disclosure. Cisco reports…

### Google Chrome browser CVE-2020-6519 Vulnerability

Google Chrome browser vulnerability (CVE-2020-6519) allows attackers to bypass the Content Security Policy on websites to steal data and execute rogue code, exposing billions to data theft, Threat Post reports…

### Microsoft August 2020 Patch fixes 120 vulnerabilities

This month Microsoft company has patched 120 vulnerabilities across 13 different products, from Edge to Windows, and from SQL Server to the .NET Framework. Among the 120 vulnerabilities fixed this month, 17 bugs have received the highest severity rating of "Critical", and there are also two zero-days — vulnerabilities that have been exploited by hackers before Microsoft was able to provide today's patches. ZDNet reports…

### WordPress Facebook Plug-in Compromising

A high severity bug found in Facebook's official chat plugin for WordPress websites allowing attackers to intercept messages sent by visitors to the vulnerable sites' owner, Bleeping Computer reports…

### Hackers Exploit Autodesk Flaw in Recent Cyberespionage Attack

Threat actors exploited a vulnerability in the popular 3D computer graphics Autodesk software in order to launch a recent cyber-espionage attack against an international architectural and video production company. Researchers said that further analysis of the attack points to a sophisticated, APT-style group that had prior knowledge of the company's security systems and used software applications, carefully planning their attack to infiltrate the company and exfiltrate data undetected. The targeted company, which researchers did not name, is known to have been collaborating in billion-dollar real estate projects in New York, London, Australia and Oman. Threat Post reports…

## Links to Cyber Related Institutions

**Links to Bulgarian, UK & International bodies**

- Secure Digital Future 21, World Economic Forum
- DSTL, DSTL Cyber Systems Programme – UK
- Ponemon Institute, Interpol
- (ISC)², Paloaltonetworks, Union for Private Economic Enterprise

## Feedback

For questions & recommendations

E-mail: acerta@bas.bg

## Editorial Board

Academic CERT association under an agreement signed from a group of academic bodies (IICT, DI, ESI as a first step) to strengthen cooperation in cyber-security related research

The publication of the newsletter is supported by the British Embassy in Sofia.
The opinions in the newsletter reflect the authors' point of view.

British Embassy Sofia

IICT Institute of Information and Communication Technologies

Bulgarian Defense Institute

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE

DIGILIENCE Conference Series
https://digilience.org