IICT
Institute of Information and Communication Technologies

Cyber-Security Newsletter

British Embassy Sofia

UK-BG Partnership in Cyber Security for SME and Organizations

Newsletter July 2020 Number 1

Aims and Scope

Contents:

- Aims and Scope
- Focus on This Issue
- The Role of CIO/CISO and COVID-pandemic Challenges
- Recommendations for the Small and Medium Organizations & Enterprises
- Presented Cyber Institution in the Issue: National Cyber Security Centre (UK) and IICT-BAS (BG)
- Useful Information about CIO/CISO and COVID-pandemic Challenges
- Links to Institutions and Initiatives
- Feedback
- Editorial Board

This online newsletter is to share timely information on COVID-related cyber threats, attacks and solutions, with focus on Bulgarian businesses and sharing best practices from the UK. The newsletter is to be published in English and Bulgarian on the official websites of the Institute of Information and Communication Technologies (IICT-BAS), the Bulgarian Academy of Sciences (BAS) and sent to contacts networks of British Embassy (BE) in Sofia.

The initiative builds on previous successful work of BE Sofia with Bulgarian key players in cyber, this project joins the efforts of the UK Science and Innovation Network (SIN), Defense and Security partnership teams in the conditions of a worldwide pandemic. The project aims at promoting the UK expertise and leadership in cyber security especially in this particular moment, and cement UK's position as a partner-of-choice to Bulgaria in cyber security. Efforts will be undertaken to strengthen the UK-BG collaboration and raise awareness on issues of mutual interest among a wide range of audiences in Bulgaria, including businesses.

In recent years and especially with the COVID-19 pandemics Small and Medium Enterprises/Micro Enterprises (SME/ME) increasingly rely on collaborative tools with adequate cyber-security to protect against increasing threats to networks, devices, and organizational and personal information. Cyber-security solutions prevent attacks to the networks and devices accessing to private information. The risk levels vary and real threats can range from sophisticated (cyber terrorism, state sponsored actors) to lower impact attacks ("script kiddies", malware etc.). What we experience anyway is that we live in more and more connected world with cyber-attacks becoming more and more frequent and dangerous.

The Newsletter is structured to introduce recent news on cyber security, related to COVID and SME/ME, present one key topic with an analytical short paper, recommend actions in the identified priority area for the issue, present some valuable resources on cyber security and introduce key institutions in Bulgaria, United Kingdom, NATO and EU, dealing with cyber security.

Editorial board is joint between IICT-BAS and partners with agreement signed for cooperation in cyber security area – Bulgarian Defense Institute (BDI) and European Software Institute – Center Eastern Europe (ESI CEE) as well as Union for Private Economic Enterprise in Bulgaria (SSI).

Every issue will have editor-in-chief introducing the main topic, so we will appreciate a feedback and proposals for the key aspects of Cyber Security for SME/ME to be addressed in the future. The first issue is under the editorial leadership of Prof. Daniela Borissova DSc., Chief Information Officer (CIO) of IICT.

Dr. Velizar Shalamanov, IICT deputy director, project leader.

Dr. Emilia Pecheva, UK Embassy in Sofia, Science and Innovation Officer for Bulgaria & Romania.

Issue Focus: The Role of CIO/CISO and COVID-Pandemic Challenges

Prof. Daniela Borissova, DSc.
CIO at IICT

The role of **Chief Information Officer** (CIO) is a relatively new and continuously evolving. The responsibilities of CIO are related to company performance, evaluation, and turnover emphasizing the management, implementation, and usability of information and computer technologies.

The CIO is focusing on analysing various technologies that the company can benefit or improve an existing business process to get reliable return of investment. One major responsibility of a contemporary CIO is to predict the future of computer technology trends that give a business an advantage over others. The day-to-day operations of maintaining a computer system generally fall on a person known as a chief operating officer of IT. Such a role is a prerequisite for success even for SME/ME in order to exploit the opportunities of the digital transformation.

What does a CIO do?

The CIO has ownership of IT and as such has responsibility for the key delivery requirements that fall to the technology department. So, in addition to contributing to the organization's overall IT strategy, the CIO:

- establishes, maintains and oversees at the highest level the technology architecture and technology choices that power the organization, ensuring that the systems are available and reliable;
- establishes and maintains the technology infrastructure in a way that aligns with the resources (i.e., budget) made available to IT for that task;
- evaluates, purchases and deploys technologies;
- sets parameters for when, where and how others within the organization can purchase, implement and deploy technology;
- optimizes technology resources – software, hardware, staff and spending – to deliver the best value and highest returns on investment to the organization;
- collaborates with the CISO and the CISO's team to ensure systems meet the organization's established cybersecurity frameworks;
- researches and evaluates existing and emerging technologies to understand where new systems can be used to achieve organizational objectives and plan for how the organization will utilize systems for its gain in the near- and far-term future

CIO and COVID-pandemic

Technology infrastructure is now more important than ever to enable business continuity and create a strong foundation for future resilience. In resume, the most important directions include:

Infrastructure revision to ensure new communication platforms that support the return to work;

Acceleration towards next-generation collaborative intelligent platforms;

Providing data security across the organization's remote workforce and support the security of suppliers, contractors, and customers.

The first direction requires to make infrastructure revision to answer if the existing infrastructure is reliable and can support all of the needed platforms for remote working. If the answer is positive a survey of the suitable platforms in accordance with the SME/organization needs is to be done. In case of a negative answer, the CIO should take some actions to hire server space that could be shared between workers. In addition, the used platforms are to be cloud-based or SaaS/cloud. There are three essential tools that should be available for each company whatever it is SME or a non-profit organization like a university. They are related to: video conferencing tools; project management (PM); learning management systems (LMS).

Video conferencing tools are becoming mandatory to connect remote teams' members including teams from business companies such as SME, non-profit organizations, universities, government, etc. These freeware or shareware tools provide connections via virtual classrooms. Some of the widely used platform for video conferencing are: Zoom, Google Meet, Cisco Webex Meetings, Microsoft Teams, Slack, GoToMeeting, etc.

The PM platforms enable the follow-up of the different ongoing projects activities. The PM software provides a flexible solution that combines different sets of tools, features, and functionalities. They help to achieve their goals by managing, tracking, communicating and reporting on project activities, time, resources, costs, and scope constraints. Many small and medium-sized businesses across all industries are now using online project management software. This type of software uses cloud-based technology and is offered by application service providers as software-as-a-service (SaaS). Some of the popular PM platforms are: Scoro, Zoho, Nifty, monday.com, ProofHub, Clarizen, Project Manager, JIRA, etc.

The LMS is focused on learning, which is the core of delivering any educational or training program by an individual. Management is the stem of the learning or training program which manages all the schedules for each and every individual. The business benefit from such LMS by providing some training courses for better understanding the systems work or to support cyber-security education and training. Some of the popular LMS are: Moodle, TalentLMS, Forma LMS, Chamilo, etc.

During the last year, the team from IICT work actively on the preparation of courses for cyber-security certification.

The third direction that CIO has to focus under COVID-pandemic is related to provide the data security across the organization's remote workforce. CIOs must keep the organization's workforce connected, collaborating, and productive, with the right tools, which are resilient, secure, and scalable. But maximizing performance and security while optimizing cost efficiencies seem impossible at this new scale. To provide the needed cyber-security, the CIOs should be in narrow cooperation with the chief information security officer.

Chief Information Security Officer

The **Chief Information Security Officer** (CISO) is the executive role for an organization's information and data security. The CISO's role is to create a strategy that deals with ever-increasing regulatory complexity, creating the policies, security architecture, processes and systems that help reduce cyber threats and keep data secure. Compliance is a key element of the role, as well as understanding risk management.

There's a list of expected technical skills that CISO should have beyond the basics of programming and system administration that any high-level tech exec would be expected to have. CISO should also understand some security-centric tech, like DNS, routing, authentication, VPN, proxy services and DDOS mitigation technologies; coding practices, ethical hacking and threat modelling; and firewall and intrusion detection/prevention protocols.

What does a CISO do?

CISOs manage the companies' overall information security. CISOs identify weaknesses within existing information security technologies and programs. Through collaborations with executives and teams of information technology security experts, these professionals develop security policies and information protection practices. They introduce new technologies, oversee education programs, and provide leadership and guidance to personnel. Additional duties include preparing budgets and financial forecasts for security operations and maintenance. CISOs also allocate financial resources, coordinate investigative and data recovery efforts, carry out risk assessments and audits, and ensure compliance with applicable regulations and laws.

CISO and COVID-pandemic

As more people are working from home during the COVID-19 pandemic, cybersecurity operations are facing tremendous new challenges. Within organizations, cybersecurity leaders need to take a stronger and more strategic leadership role. They need to move beyond being compliance monitors and enforcers to better integrate with the business, manage information risks more strategically and work toward a culture of shared cyber-risk ownership across the enterprise. The following questions will foster effective conversations between business leaders and CISOs:

- Have roles and responsibilities related to cybersecurity been clearly defined and communicated at every level of the organization up to the CEO and Board?
- Do business leaders understand the cybersecurity risks they are accepting?
- Are technology solutions designed, integrated and operated with security and privacy in mind?
- Does the business incentivize the adoption of secure-by-design-and default practices on the businesses and products in which it invests?
- Are third-party risks managed effectively?

The daunting challenge for CISOs is protecting the organization's digital infrastructure and assets while enabling operations without interruption. For example, cybersecurity teams must adjust security programs and risk management practices to enable the massive shift to work-from-home tools and fast adoption of cloud services.

Data Protection Officer

What does a DPO do?

Along with CIO and CSIO, any company (business or non-profit) should have a Data Protection Officer (DPO). DPO is a security leadership role required by the General Data Protection Regulation (GDPR). DPO is responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements.

The DPO is a mandatory role for all companies that collect or process EU citizens' personal data, under Article 37 of GDPR. DPOs are responsible for educating the company and its employees about compliance, training staff involved in data processing, and conducting regular security audits. DPOs also serve as the point of contact between the company and any Supervisory Authorities (SAs) that oversee activities related to data.

If you don't have someone with the role of CIO/CISO/DPO – it is probably wise to assign these responsibilities to an executive team member or organize these activities through kind of shared services/outsourcing with other SME/Organizations.

Recommendations for the Small and Medium Organizations & Enterprises

COVID-19: Moving Your Business from the Physical to the Digital

Moving your business online will present some new risks. The first thing to do is establish what these are.

New dependencies: Working online will inevitably mean placing more reliance on digital technology, including online services such as web hosting, credit card processing and productivity tools like email, video and chat. Are your existing arrangements able to accommodate increases in use and reliance? For example, do you have the necessary bandwidth to handle increased web traffic? Do you have sufficient online storage capacity? Are you regularly backing up your essential data? Do you have access to IT support?

Check the service agreements: For services you already have in place, there may be Service Level Agreements (SLAs) or contractual arrangements involved. It's worth reading these to be sure you have the resources in place that you think you do.

Assessing the Cyber Security of the Business	Online security is important, but it should be considered in the context of your overall business needs. Start by considering whether the measures you take to deal with the COVID-19 lockdown will become more permanent ways of working. For example, will you allow homeworking to continue, will you look to expand your online business? If so, you will need systems in place which are sustainable and can scale as your business adapts and grows. Cloud services have been designed to meet this need, allowing you to grow or shrink your IT requirements in response to market conditions, without massive investment in hardware or personnel. They have many advantages in terms of security, but you as an end user will still be ultimately responsible for your data, how this is accessed and by whom
What Technology Do You Use Already?	What IT assets do you own, operate and manage yourself? It's difficult to secure technology if you can't identify who's responsible. Is it your job exclusively? Your service provider's? Or a joint effort? Clarity is the important thing here.
Do You Have Success to IT Support?	As you become more reliant on digital services to do business, you should think about how you'd cope if these services became unavailable. Detailing the services you use, identifying support levels and escalation routes, will help you understand and prepare for any issues.
What Cyber Security Measures Do You Have in Place?	In UK, the NCSC's Small Business Guide can help you to establish a baseline set of security policies for your IT. Cyber Essentials provides a way to demonstrate to others that you have good security in place.
Are There any Regulations You Need to Follow?	Rules are rules, even on the Internet. If your business is now processing Personally Identifiable Information (PII) online, you will need to read up on GDPR. If you are processing card payment information, the Payment Card Industry Data Security Standard will apply. Be clear on the balance of legal and regulatory responsibility between you and your IT service providers.
Do you Have Cyber Insurance?	Are any elements of it affected by your change in circumstances, such as working from home, running a predominately 'online' business, or by outsourcing key business functionality?
If You Are Talking Directly with Your Supplier, Focus on These Security Issues	**Patching and updates:** It is vitally important that Internet and cloud service providers keep software updated, and apply the latest security patches as soon as they become available. Ask your suppliers how often they patch the services you use, and check any contracts or SLAs to ensure that patching is included. **Backups:** What sort of backup arrangements are in place and how often are these tested? If the service provider was, for example, to suffer a ransomware attack, how would they recover their service and your data? You should determine how often your data is backed up, where it is stored, and who has access to it. **Access:** Is your data, and the data of others you are responsible for, being properly protected? Are you able to put two-factor authentication in place to limit access to your data and services? The NCSC also provides guidance on two of the most common encryption solutions used for protecting data across the Internet: TLS and IPsec. **Logs:** Are logs being kept for security purposes? Logging can play a vital role in diagnosing any problems your systems are facing. Logs will also prove invaluable when responding to and recovering from security incidents. **Incident Response:** What will happen if things go wrong? Service providers should operate on the presumption that they will be attacked. It should be clear how and when they will engage with you during a security incident.
Security as a Foundation for Future Growth	Moving your business from the physical to the digital securely will not only help your business grow confidently and sustainably, but it will also help to uphold your reputation with customers. It's important to keep the

	dialogue open with your IT service providers, building a positive relationship and developing a better understanding of each other's responsibilities.

Cyber Institutions in UK & Bulgaria

National Cyber Security Centre **National Cyber Security Centre (NCSC) – UK** **What does NCSC do?**	NCSC supports the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, NCSC provides effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future. More specifically, the NCSC: • understands cyber security, and distils this knowledge into practical guidance that we make available to all • responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK • uses industry and academic expertise to nurture the UK's cyber security capability • reduces risks to the UK by securing public and private sector networks
History of the NCSC	Launched in October 2016, the NCSC has headquarters in London and brought together expertise from CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure. The NCSC provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments. We also work collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners.
Covid-19 and Cyber Security	Over the last months, the UK NCSC has issued a lot of material relating to cyber security in the context of Covid-19. Including: • A joint advisory with US and Canadian equivalent agencies, • Guidance for organisations with staff working from home and on how to identify phishing emails related to Covid, • Guidance for organisations on how best to select, configure and securely implement video conferencing services.
Practical information for SMEs	Advice & guidance
IICT **Institute of Information and Communication Technologies at Bulgarian Academy of Sciences (IICT-BAS) – BG**	The **IICT-BAS** is founded on 1 of July 2010 as a successor of Institute for Parallel Processing, Institute of Information Technologies and Institute of Computer and Communication Systems. The research and development activities of the IICT covers the following directions: Artificial intelligence and language technologies; Communication systems and services; Information technology in security; Information technologies for sensory data processing; Information processes and decision making systems; Intelligent systems; Parallel algorithms; Modelling and optimization; Scientific calculations with Laboratory of 3D digitalization and microstructural analysis; Scalable algorithms and applications with Center for High Performance Computing; Distributed information and management systems; Cyber-physical systems.

Useful Information about CIO/CISO and COVID-pandemic Challenges

Coronavirus (COVID-19) Outbreak: Short- and Long-Term Actions for CIOs	CIOs need to increase resilience against future disruptions, and prepare for rebound and growth. While organizations may be in a crisis mode to cope with short-term impacts, there are long-term impacts that they should be aware of. When traditional channels and operations are impacted by the outbreak, the value of digital channels, products, and operations become immediately obvious and CIOs can present a more convincing business case. This is a wake-up call for organizations that focus on daily operational needs at the expense of investing in digital business and long-term resilience.

COVID-19: Insights for CIOs and IT Executives	Technology executives all have vital roles to play in steering their organization and teams to function effectively through the COVID-19 crisis. This has a real impact on every area of the enterprise, from operational to financial – to technical and personal. To help address these impacts, KPMG has developed a list of immediate, medium- and long-term considerations that you as an IT leader might consider as you tackle supporting your company through these challenging times.
Successful Digital Transformation Requires Data Transformation	Whether or not an organization has launched a formal digital transformation initiative, there's no doubt most business operations are now inseparable from the IT infrastructure on which they run. As a result, technological advances, if properly managed, can translate directly into business advances. Many companies are struggling to bridge the gap that exists between their existing IT infrastructures and practices and the value that new digital technologies make possible. Fortunately, there is a clear way to optimize digital transformation efforts: focus on the data. Digital transformation is likely to fall short unless it is based on a solid foundation of "data transformation".
CIO Management Toolkit 2020: COVID-19 Significantly Alters the Priorities for CIOs as CFOs Begin to Adjust to Impacts on the Way Companies Now Operate	CIOs and CTOs are in a constantly evolving field, however, world-class CIOs and CTOs focus on three areas to help them manage more effectively. They are: *Technology; People; Infrastructure*. The top 11 concerns are the areas of focus for CIO and enterprises: access management; work from home; mobile computing; blockchain; social media impact; security and hacking; staffing; skills for new technologies; risk management; data privacy; ROI on new technology.
How Technology Leaders are Responding to the COVID-19 Crisis	The pandemic has accelerated the pace of digital transformation and technology is playing a pivotal role in reshaping business. Our survey data shows that investing in digital customer experience requirements and new technology enabled business models remain top priorities for CIOs in 2020 as well as 2021. At the same time IT infrastructure investments are needed in the area of cybersecurity and digital workplace tools. Balancing investments in internal IT infrastructure and external, customer focused, digital capabilities, while optimizing their IT spending is a major challenge facing CIOs today.
Coronavirus: CIOs Should Consider a New Desktop IT Strategy	Ranjit Atwal, senior research director at Gartner, noted that the topline forecast from Gartner paints a depressing picture for the market. In its latest device market forecast, the analyst firm predicted that PC sales would decline by 10%, while smartphones would decline by 14.6%. Gartner's forecast estimates that 48% of employees will likely work remotely at least part of the time after the coronavirus pandemic, compared to 30% pre-pandemic. This trend will make business notebooks displace desk-based PCs through 2021 and 2022.
ECSO Barometer 2020: "CYBERSECURITY IN LIGHT OF COVID-19"	From March to May 2020, the European Cyber Security Organisation (ECSO) conducted surveys with its members and the cybersecurity community (large companies, RTO's/universities, regions/clusters, SME's, public administrations, EU institutions/agencies, users/operators, and associations) in order to better understand the impact of the COVID-19 pandemic on the activity of cybersecurity stakeholders during the crisis period, as well as their expected challenges post-crisis.
Cyber Security Response Package available to the Business and Healthcare Providers	In the hight of the Covid-19 pandemic, the European Cyber Security Organization introduced a Covid-19 Cyber Security Response Package. The document compiles rapid response initiatives / tools / services from the European cybersecurity community which includes ECSO members, ECSO partners, and other stakeholders. It is regularly updated with input received from the community, as part of our Cyber Solidarity Campaign. The efforts are presented in 5 domains: 1) Resources for the healthcare sector; 2) General COVID-19 resources; 3) National/regional initiatives; 4) Working from home; 5) Cyber-attacks during COVID-19.

Post-COVID-19: A CIO Recovery Guide – Scenario Planning your Responses	Most CIOs never had a scenario for a COVID-19 pandemic. In a period of uncertainty, it is impossible to predict the future; however, it is important to evaluate the range of possibilities. The goal is not to be able to play all the scenarios but to become more agile and be ready to adapt to a new scenario, even an unanticipated one. In a period of uncertainty, not doing anything is a decision with a cost and with consequences. Some are direct and immediate consequences; long-term effects may be more significant and are far more difficult to predict.
COVID-19 Action Guide: Beyond the Great Lockdown	This special report provides such a framework, organized around seven key imperatives that will be useful for any organization's executive team. These seven areas are: empower a remote workforce; engage customers virtually; remote access to everything; accelerate agility and efficiency; protect against new cybersecurity risks; reduce operational costs and enhance supply chain continuity; support health providers and government services.
How Remote Work is Changing CIO Priorities Amid the COVID-19 Pandemic	The survey, which was conducted in mid-March with more than 200 CIO respondents in the US, highlights the biggest priorities and challenges facing technology leaders and where they plan to invest in the future. Unsurprisingly, the area of cyber-security is a major CIO priority in the pandemic and post-pandemic world, with 7 in 10 organizations expecting to increase their financial investments in security technologies. Public cloud, infrastructure, and AI and machine learning will also receive financial boosts in many organizations, the survey found.

Links to Institutions and Initiatives

Links to Bulgarian, UK, EU and NATO Bodies & Initiatives	• IICT-BAS • National Cyber Security Centre (UK) • Union for Private Economic Enterprise • Cyberwatching.eu • NCIA/Cyber Security Center • DIGILIENCE 2020

Feedback

For questions & recommendations	E-mail: acerta@bas.bg

Editorial Board

Academic CERT Association (**ACERTA**) 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	1. Dr. Velizar Shalamanov – Deputy Director of IICT-BAS 2. Dr. Todor Tagarev – IICT-BAS 3. DSc. Daniela Borissova – CIO at IICT-BAS 4. Dr. Zlatogor Minchev – CISO at IICT-BAS 5. Dr. Nikolay Stoianov – Deputy Director of Defense Institute at Ministry of Defense 6. Dr. George Sharkov – Director of European Software Institute – Center Eastern Europe 7. Svetlin Iliev – Union for Private Economic Enterprise

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