

IV Investors' Voice

The American Chamber of Commerce in Kazakhstan

Kazakhstan's Leading International Business Association



December 2019
HOLIDAY ISSUE

www.amcham.kz

#86

Cybersecurity and Cybercrime A 21st Century Challenge



- ▶ Kazakhstan's Digitalization and Cybersecurity Strategy
- ▶ Why Cybersecurity Matters
- ▶ State-of-the-Art Cybersecurity
- ▶ Creating a Healthy and Safe Digital Ecosystem for the Future
- ▶ Being Secure in the Transition to 5G
- ▶ Oracle's Contribution to Cybersecurity
- ▶ Cybersecurity for the Oil and Gas Industry

Мерекені
жақындарыңмен
өткіз

Раздели
праздник
с близкими



ТАТЫП КӨР... СЕЗІН
ПОПРОБУЙ... ПОЧУВСТВУЙ



Тауар декларацияланған. КО сәйкестік туралы декларациясының тіркеу нөмірі № KZ.7500317.24.01.27947
«СОСА-СОЛА», «СОКЕ», «СОКЕ ZERO», КОНТУРЛЫ БӨТЕЛКЕ ЖӘНЕ СЕРПІНДІ ТОЛҚЫН THE СОСА-COLA COMPANY (ДЗЕ КОКА-КОЛА КОМПАНИИ)
КОМПАНИЯСЫНЫҢ ТІРКЕЛГЕН ТАУАР БЕЛГІЛЕРІ. © 2019 Тауар декларацияланған.
«СОСА-СОЛА», «СОКЕ», «СОКЕ ZERO», КОНТУРНАЯ БУТЫЛКА И ДИНАМИЧЕСКАЯ ВОЛНА ЯВЛЯЮТСЯ ЗАРЕГИСТРИРОВАННЫМИ
ТОВАРНЫМИ ЗНАКАМИ КОМПАНИИ THE СОСА-COLA COMPANY (ДЗЕ КОКА-КОЛА КОМПАНИИ). © 2019 Товар задекларирован.

Admissions
now open for
2020-2021

Why choose Haileybury?

Pathway to the world elite universities
(Ivy League in USA, Russell Group in UK).

Highly qualified British teachers.

An excellent learning environment,
which allows children
to grow academically and holistically.

Haileybury Astana

admissions@haileyburyastana.kz

+7 (7172) 55 98 55 (ext. 122)

    HaileyburyAstana



www.haileybury.kz

Haileybury Almaty

admissions@haileyburyalmaty.kz

+7 (727) 355 01 00 (ext. 240)

    HaileyburyAlmaty

ALMATY

AKTOBE

FLY

WE ARE NOTHING
WITHOUT YOUR SMILE



FlyArystan



air astana

EDITOR'S NOTE



Dear Readers,

As the year draws to a close, the *Winter Holiday Issue of Investors' Voice* is always an important publication for AmCham as we plan for the year ahead and look back at the accomplishments of the past year. 2019 has been an intense year for AmCham and for Kazakhstan as the country undergoes a political transition that is still unfolding. The unexpected announcement in March that President Nazarbayev would step down triggered the appointment, and in June the election of a new President, Kasym-Jomart Tokayev. The Government announced business as usual, but AmCham members and AmCham itself took a deep breath as we sought to understand the new political landscape.

AmCham took a short break in the *Prime Minister's Council to Improve the Investment Climate* as the new Prime Minister and newly-appointed Cabinet settled into their roles. In the autumn, the Council resumed with a new set of topics for consideration by the Government. The October topic was Cybersecurity, a subject the Government treated as a high priority, given its current Digitalization Initiative to modernize Kazakhstan's communications system.

Following on the Council Cybersecurity session, AmCham organized a Conference on the expanded theme of *Cybersecurity and Cybercrime: A 21st Century Challenge*, which served to bring the discussion into the public arena. Keynote Speakers were the *Minister of Digitalization and Innovation, Minister of Justice*, and the *Ambassadors of the United States and Canada*. Speakers throughout the Conference were corporate CEOs and cyberexperts, many of whom had travelled from abroad to participate in the Conference.

The present Issue of *Investors' Voice* is devoted to the Conference presentations, which examined the challenges posed by Cybersecurity from the perspective of leading companies – *Microsoft, Oracle, Ericsson, Honeywell, NCOC, Mastercard, Citibank*, law firms and the Big Four audit firms, each providing analysis and recommendations for the future.

We therefore offer readers of the *December Investors' Voice* thought-provoking articles and political developments as we look back on 2019 and forward into 2020. Time does not stand still, and the New Year will be as challenging and as exciting as the year that is now ending.

With All Best Wishes for the New Year,
Doris Bradbury, Editor-in-Chief

TABLE OF CONTENTS

Cover Art: Birds Seeking Fruit by
Fred Tomaselli

ARTICLES

Cybersecurity and Cybercrime: A 21 st Century Challenge Conference Overview.....	9	Cybersecurity for the Oil & Gas Industry Ivo Aalbers.....	22
Keynote Speech by U.S. Ambassador to Kazakhstan William Moser.....	14	Cyber Crisis Management: Readiness, Response, Recovery Vladimir Remyga.....	23
Keynote Speech by Canadian Ambassador to Kazakhstan Nicholas Brousseau.....	15	Being Secure in the Transition to 5G Aidyn Abjanbekov.....	29
Keynote Speech by Ambassador of the Netherlands André Carstens.....	17	Cybersecurity for Business and Public Services Andrey Gusakov.....	30
Keynote Speech by Minister of Digitalization and Innovation Askar Zhumagaliyev	18	Cybersecurity for Mobile Operators in Kazakhstan Kaspars Kukelis.....	32
Keynote Speech by Minister of Justice Marat Beketayev.....	18	Introducing Digital Trust Insights Vitaly Sokolov.....	34
Intellectual Property and Cybersecurity Andrei Yorsh.....	19	Chamber Events.....	38
Creating a Healthy and Safe Digital Ecosystem Piotr Marczuk.....	20	Member News.....	50
		Member Profiles.....	54
		Advocacy Update.....	55
		Working Group Update.....	57

BOARD OF DIRECTORS

CREDITS

EDITOR IN CHIEF:

Doris Bradbury

COVER ARTWORK:

Birds Seeking Fruit

CONTRIBUTORS:

Ivo Aalbers

Aidyn Abjanbekov

Marat Beketayev

Nicholas Brousseau

André Carstens

Andrey Gusakov

Kaspars Kukelis

Piotr Marczuk

William Moser

Vladimir Remyga

Vitaliy Sokolov

Andrei Yorsh

Askar Zhumagaliyev

PUBLISHER:

**American Chamber
of Commerce in Kazakhstan**

Tel.: +7 (727) 330 92 50

Fax: +7 (727) 330 92 51

EXECUTIVE COMMITTEE



Kenneth Mack
President
Principal
Mack Law



Bela Ferenczi
Vice-President
CEO
General Electric



Paul Cohn
Treasurer
Partner
EY



Ashley Clarke
Secretary
Chief Operating Officer
KPMG

BOARD MEMBERS



Doris Bradbury
Executive Director
AmCham



John Baltz
Managing Director
Eurasia Business Unit
Chevron



Tibor Kolejak
Country Manager
Microsoft Kazakhstan



Dean Matlack
Commercial Counselor
U.S. Consulate General
in Almaty



Olga Voronova
Country Manager
Procter and Gamble



Gani Uzbekov
Founder and CEO
SILK



Saule Zhakayeva
Deputy Chair
Corporate Banking Head
Citi Bank

For information about the AmCham, please email info@amcham.kz
For information about Investors' Voice and the Chamber's website,
please email Anar Zholdoshbek kyzy at Anar.Zholdoshbek.kyzy@amcham.kz
To enquire about financial issues,
please contact Rimma Kazhemyakina at Rimma.Kazhemyakina@amcham.kz

CONTRIBUTORS

Embassy of the United States



William Moser, Ambassador of the United States

William Moser was confirmed as US Ambassador to Kazakhstan on January 2, 2019 after serving as US Ambassador to Moldova. Since entering the diplomatic corps in 1984, he served in Ukraine, Egypt, Suriname, Mali. State-side he served as Deputy Executive Director for European and Eurasian Affairs, Post Management Officer in the Bureau of Near Eastern and South Asian Affairs, and Political-Military Affairs Officer in the Bureau of Political Military Affairs.

Ambassador Moser has won numerous commendations including the Secretary of Defense's Medal for Distinguished Civilian Service and the Leamon R. Hunt Award for Management Excellence. He holds a B.A. in Political Science from the University of North Carolina at Chapel Hill.

Embassy of Canada



Nicholas Brousseau, Ambassador of Canada

Nicholas Brousseau was appointed Canada's Ambassador to Kazakhstan, the Kyrgyz Republic and Tajikistan in 2017. He joined Foreign Affairs Canada (now Global Affairs Canada) in 2004, where he was assigned to the European Union Division and later to the Eastern Europe and Balkans Division. He served as Deputy Director of the Department of Arms Control and Disarmament and at the Permanent Mission of Canada to the UN. Abroad he was assigned to the Canadian Embassy in Russia and Romania. Prior to his appointment as Ambassador, he served as Senior Adviser to the Minister of Foreign Affairs.

Nicholas Brousseau received his B.A. in History at Laval University and an M.A. and Ph.D. in History from the University of Paris 1 Pantheon-Sorbonne.

Embassy of the Netherlands



André Carstens, Ambassador of the Netherlands

André Carstens is Ambassador of the Netherlands to Kazakhstan, Kyrgyzstan, and Tajikistan. A long-serving public servant with previous international posts in Russia, Georgia, and in Afghanistan, he rose to senior positions in the Netherlands' Ministry of Foreign Affairs and the Ministry for Security and Justice. Notably, he headed the Netherlands' contribution to the EU Monitoring Mission in Georgia and served as Director of Governance in Mazar-e Sharif, Afghanistan. Prior to his current position, he served as Advisor to the European Counterterrorism Coordinator in Brussels.

André Carstens received his Master's degree in Social-Economic Law from the University of Utrecht, and completed diplomatic training for the Ministry of Foreign Affairs and the Senior Leadership Program of the Netherlands General Public Service.

Government of Kazakhstan



Askar Zhumagaliyev, Minister of Digitalization and Innovation of Kazakhstan

Askar Zhumagaliyev is Minister of Digital Development and Innovations Kazakhstan. Minister Zhumagaliyev's career in public service has covered senior positions in Ministries focused on communications, information, technology, and development, and from 2006-2010 he served as Chairman of Kazakhtelecom. From 2017-2019 he was Deputy Prime Minister of Kazakhstan, and from 2018-2019 he served as Deputy Minister of Defense.

Minister Zhumagaliyev graduated from Kazakh National Technical University, specializing in radio communication, broadcasting, and television. He received a Law degree from Kazakh Humanitarian University and a Master's degree in electronic governance from Polytechnic of Lausanne in Switzerland.



Marat Beketayev, Minister of Justice of Kazakhstan

Marat Beketayev is Minister of Justice of Kazakhstan. He began his public service career soon after completing his university education. From 2001 - 2003 he served in the Ministry of Foreign Affairs in the field of information processing and analysis. He then was promoted to senior positions as Deputy Director for State Enterprise, Advisor to the Deputy Prime Minister, Advisor to the Prime Minister, Deputy Minister of Justice, Executive Secretary at the Justice Ministry and, prior to his current position, he served as Deputy Head of the Presidential Administration.

Minister Beketayev is a graduate of Kazakh State Law University and the London School of Economics and Political Sciences.

Baker McKenzie



Andrei Yorsh, Partner, Baker McKenzie Law Firm

Andrei Yorsh is a Partner at the Almaty office of Baker & McKenzie. He specializes in dispute resolution, intellectual property, and labor law. He also has extensive experience in healthcare and pharmaceuticals, corporate law, mergers and acquisitions and antitrust & competition issues. He is recommended by Legal 500 EMEA and Chambers Global and is ranked as a leading lawyer in his field.

Mr. Yorsh graduated with honors from Belarusian State University and was admitted to practice in 1994. In 1997, Mr. Yorsh completed a post-graduate course at Belarusian State University. He is an international arbitrator for the Belarusian Chambers of Commerce.

Deloitte



Vladimir Remyga, Director, Risk Advisory, Deloitte Kazakhstan

With over twenty years of experience in IT and cyber security field, Vladimir Remyga leads Deloitte's digital and cyber security services in the Caspian and Caucasus regions. He serves clients throughout the CIS and specializes in digital and cyber risk management, IT cost optimization, and digital transformation. Prior to his current position at Deloitte, he was IT Advisory Director at KPMG and Senior Manager and Executive Director at EY.

Vladimir Remyga received an Honors B.A. in Information Defense and Protection from Kazakh National Technical University and an MBA from Moscow International Business School.

CONTRIBUTORS

Ericsson



Aidyn Abjanbekov, General Director, Ericsson Kazakhstan

Aidyn Abjanbekov is CEO of Ericsson in Central Asia and Mongolia. He is responsible for strengthening the company's technological leadership through development of mobile broadband, 5G, IoT, cloud, digitalization and cyber security technologies. Mr. Abjanbekov joined Ericsson in 2011, holding various senior positions in Sweden and Russia. Prior to his current position, he served as Ericsson's Vice President for Government Relations for Russia and the CIS. Before Ericsson, he worked in telecommunications, consulting, and in Ministries of Communications abroad with a focus on strategic management, infrastructure development, and operational efficiency.

Aidyn Abjanbekov received his M.A. in Business Administration from the University of Linköping in Sweden.

KCELL



Kaspars Kukelis, CEO, KCELL

Kaspars Kukelis has over twenty years of experience in the telecommunications industry, having held various senior-level management positions at a variety of companies. Before returning to Kcell in 2019 as CEO, he served as the Senior Retail Director at Kazakhtelecom and was a member of its Management Board. He also served as an Independent Director at Altel and was Kcell's Marketing Director, after which he was promoted to become its Chief Commercial Officer.

Kaspars Kukelis graduated with a degree in Economics from the Kazakhstan State Academy of Management and holds an EMBA degree from Harvard Business School. He also serves as the Honorary Consul of Latvia.

Microsoft



Piotr Marczuk, Corporate Director for Microsoft Central/Eastern Europe, Microsoft

Piotr Marczuk is Government Affairs Manager for Microsoft based in Poland. He joined Microsoft in 2008 and specialises in engaging with government officials, regulators, policy makers, and industry groups in Poland. He also co-ordinates these relationships in Estonia, Latvia, Lithuania, and Ukraine. Mr. Marczuk began his career working in the Polish government and, prior to joining Microsoft, worked in Government Affairs for British American Tobacco.

Piotr Marczuk received a B.A. and Master's degree in Law from the Maria Curie Skłodowska University in Lublin, Poland.

North Caspian Operating Company (NCOC)



Ivo Aalbers, General Manager, IMT/IT, North Caspian Operating Company (NCOC)

Ivo Aalbers serves as Chief Information Officer for NCOC, which operates the Kashagan oil field. He has over 20 years of experience in IT management since he began as Senior Information Planner at Brunei Shell Petroleum. He worked for Shell for two decades in various leadership positions as Lead IT Consultant, Production and Engineering IMT/IT Manager, and, prior to joining NCOC in 2018, as Shell's Data Integration Manager.

Ivo Aalbers received his Master's degree in Arabic Language and Culture from Leiden University, a Master's degree in Business Administration from Erasmus University, and Certificates in the Business Leadership Program and Strategic Business Partnerships from IMD Business School.

Oracle



Andrey Gusakov, Head of Information Security Technology Consulting, Oracle CIS

Andrei Gusakov has worked at Oracle since 2006, beginning as a Senior Consultant. He currently leads consulting teams in Information Security throughout the CIS. His specialty is data protection, whether internal, external, cloud, or corporate data. Prior to joining Oracle, he was A.T. Kearney's IT Specialist, Sakhalin Oil's Senior IT Specialist, and IBM Eastern Europe/Asia Pre-Sales Specialist.

Andrey Gusakov is a graduate of the National Science and Technology University in Moscow.

PricewaterhouseCoopers



Vitaliy Sokolov, Partner, Advisory Service, PwC Russia

Vitaly Sokolov leads PwC's cybersecurity practice in Russia and Eurasia. With over 20 years of experience in the field, he specializes in addressing complex cybersecurity challenges in an environment with rapidly evolving threats. Prior to joining PwC, he was a Partner at a Big 4 advisory firm in Canada, where he led the national cybersecurity team in the energy sector. Before that, he was responsible for cybersecurity in one of the largest North American energy companies, where he created a cyber risk management program.

Vitaly Sokolov graduated from the London School of Economics and is a Certified Information Security Professional (CISSP), a Certified Information Systems Auditor (CISA), and a Certified Information Security Manager (CISM).

CYBERSECURITY AND CYBERCRIME: A 21ST CENTURY CHALLENGE CONFERENCE OVERVIEW

CONFERENCE SPONSORS: MICROSOFT, ERICSSON, AND MASTERCARD

The *AmCham Economic Policy Forum* is an annual Conference, which has been held consistently for over ten years in both Almaty and Nur-Sultan (Astana). The Conferences have a variety of themes and are aimed at a priority topic for Government and investors alike in a given year. Past Conference topics have included *Regional Economic Integration, Banking Regulatory Reform, Healthcare Reform, Intellectual Property Rights, Judicial Reform, Rule of Law, and Challenges to Kazakhstan's Economic Diversification*. Topics are often chosen in connection with investment policy issues discussed at the monthly *Prime Minister's Council to Improve the Investment Climate*, a Council created for AmCham ten years ago, chaired by current Prime Minister Askar Mamin and attended by Cabinet Ministers.

The October 2019 *AmCham Economic Policy Forum Conference*, entitled *Cybersecurity and Cybercrime: a 21st Century Challenge*, aimed to connect the interests of Kazakhstan's government with its allies in the fight against cybercrime and with private-sector stakeholders in the country. The Conference was held at the Marriott Astana Hotel in Nur-Sultan on the 23 October. Throughout the day, from the Keynote Addresses to the four panel sessions, Kazakhstani Government officials, foreign diplomats, CEOs, lawyers, and finance experts presented their research, their solutions, and engaged in discussions with one another.

As always, the media attended in force to report on the Keynote Addresses and to interview the Ambassadors and Ministers who opened the Conference. Reports were carried on the Prime Minister's website, in the electronic media, in the leading business print media, and on video. The concentration of officials, experts, and executives is a testament to the global importance Cybersecurity has acquired. Cybercrime is considered one of the top risks to global security in general, and Kazakhstan's political and economic growth makes it a prime target for fraud, data theft, and other criminal activity by malicious state and non-state actors.

Opening the Conference, **Tibor Kolejak, Microsoft Kazakhstan's Director**, welcomed the participants, highlighting the importance of the topic and the expertise of the speakers who would be heard throughout the day on four thematic Panels. Following his opening remarks, the four Keynote Speakers took the microphone in sequence to contribute their perspectives on the Conference topic.

The first Keynote Speaker was **Deputy Minister Askhat Orazbek from the newly created Ministry of Digitalization and Innovation**. As his department is directly responsible for development of *Digital Kazakhstan*, a current

government priority, he outlined the need for a secure digital front to protect and advance this e-governance project aimed at helping the Government serve its citizens more efficiently. He also stressed the need for the Government to take the lead in this endeavor, calling it a "catalyst" for innovation with partnerships in the private sector.

Following the first speaker, **Deputy Minister Akerke Akhmetova from the Ministry of Justice** outlined the role of the Justice Ministry in protecting Cybersecurity and tracking Cybercrime. The Ministry is responsible for the application of laws governing the internet, telecommunications, and information technologies, and must protect the privacy of sensitive data that it stores and uses for legal proceedings. The Deputy Minister agreed with the previous Speaker that the Government will play a leading role in this digital ecosystem.



U.S. Ambassador William Moser followed, delivering the position of the U.S. government concerning cybersecurity and the security of its allies given the disruptive nature of recent trends in Cybersecurity threats. As one of the largest targets in the world for cyberattacks in both the public and private sectors, the United States has a vested interest in promoting Cybersecurity awareness worldwide. He noted the Embassy's recent Cybersecurity Symposium at Nazarbaev University where local talent met with American cyberexperts to discuss Kazakhstan's challenges.

Ambassador Moser stressed Microsoft's concern about the dangers of using "under-licensed" and pirated software. Not only is this an intellectual property rights issue, but it is also a vulnerability and attack vector for malware and various other forms of cybersecurity threats. The usage of pirated software and other technology by many Kazakhstani businesses and Government agencies, heightened by the *Digital Kazakhstan* initiative leaves the country open to cyberattacks for a variety of purposes by cybercriminals. In conclusion, the Ambassador reaffirmed the U.S. government's commitment to society-wide cyber-awareness with the help of U.S. programs and consultations.



Nicholas Brousseau, Canada's Ambassador to Kazakhstan, was the final Keynote Speaker. Ambassador Brousseau outlined his Government's solutions to Cybersecurity issues, given that Canada is the world's third most-targeted country for cyberattacks. He also reported on six conclusions from Canada's *National Cyber Security Threat Assessments* review by the *Canadian Center for Cyber Security*. The Review's conclusions generally portray the constantly evolving threats, targets, motives, and means as non-state actors give way to state-sponsored attacks; how personal data becomes increasingly digitalized; and how the number of attack vectors increases with the pace of innovations that undermine older cybersecurity measures.

Canada's approach to cybersecurity is a more broadly-distributed system with coordination between fifteen government agencies. Canada's strict privacy laws protect its citizens' personal data by requiring consent from individuals that limits usage of their specific data to the expressed purposes for its collection. This law also provides legal and financial pressures on companies to better secure data from confidentiality breaches. Referring to *Digital Kazakhstan*, Ambassador Brousseau also expressed his Government's readiness to provide whatever assistance Kazakhstan might require to strengthen its Cybersecurity.

Morning Session – Panel I Cybercrime: A Growth Industry

André Carstens, Ambassador of the Netherlands to Kazakhstan, served as the first Morning Panel's moderator, also delivering a presentation on *State-of-the-Art Cybersecurity*. Ambassador Carstens outlined four major emerging cyberthreats that endanger global stability: the devastation that cyberattacks can cause by disrupting entire economies, the rise of state-sponsored cyberattacks, the ability to affect the opinions of a polity in another country's democratic society, and the use of cyberattacks as a means of "non-violent" coercive force.

He highlighted the Netherlands' commitment to cybersecurity through its recent hosting of the *Global Conference on Cyberspace* and development of its *National Cyber*

Security Strategy (NCSS). Member-countries at the Global Conference all benefit through cooperation and information-sharing that serve to "strengthen the ecosystem."

Ambassador Carstens' concluding remarks on Cybersecurity in the maritime sector stressed the crucial nature of protecting the Netherlands as a maritime economy, but also the economies of all nations in that disruptions to international sea-trade would have knock-on effects across national borders.



Ambassador of the Netherlands André Carstens

Andrei Yorsh, a Partner at Baker McKenzie Law Firm and an expert on Intellectual Property, delivered a presentation on *Intellectual Property, An Essential Component in Cybercrime*. He noted the alarming rate at which cyberattacks occur – one every 14 seconds – and that these attacks are responsible for data leaks that constitute 3 trillion USD in losses every year. At the root of it all is a failure to protect intellectual property (IP) rights. He pointed out that Kazakhstan lacked strong legislation to enforce IP rights for Government procurement, and that such legislation is an urgent need for cybersecurity and for many other purposes that protect the population in their everyday lives. Not only will protecting IP rights prove beneficial from a legal standpoint, but using licensed and protected programming, operating systems, and components will better safeguard everyone against attacks.

Igor Volkov, Director of Cyber and Intelligence Solutions at Mastercard delivered a presentation on *Financial and Credit Card Crime*. As the Mastercard representative, Mr. Volkov stressed the necessity of improved cybersecurity measures for business, banking, and finance. Referring to financial losses from cyberattacks, his presentation also outlined the long-term negative effects that such incidents have on corporate economic performance and client trust.

In response to these real threats, Mr. Volkov presented Mastercard's approach to protect itself from future attacks, embodied by three steps: *defense, identification, and detection*. On defense, Mastercard is developing more resilient infrastructure and authentication measures that

include device location identification, passive biometric identification, behavioral analytics, and a real-time *Trust Consortium*.

Concerning identification, Mastercard is integrating biometric security (such as fingerprint and facial recognition) to augment other traditional gateway security measures. On detection measures, there are active fraud alert systems that assess transaction risks during authentication procedures. Together, these measures better protect client identity and financial transactions.

Bolat Assylkhanov, a Partner at Grata Law Firm, spoke about *Cybercrime – Threats and Mitigation*. Mr. Assylkhanov focused on new vulnerabilities through proliferation of unlicensed programs – new computers sold on the market with unlicensed operating systems. In response to modern vulnerabilities, he proposes seven recommendations.

First, the latest version of a computer's operating system should always be used and computer updates must be accepted as soon as they are offered. *Second*, be wary of downloads and links from emails – even if they stem from a known address. *Third*, check URLs for spelling errors as fake sites will often mimic trusted ones. *Fourth*, never use public Wi-fi to conduct online banking as this is a vulnerable attack vector. *Fifth*, upon receiving a suspicious email from a known source, contact the sender through alternative means for confirmation. *Sixth*, use only safe “https” sites. *Last*, if accessing an unsecure resource is unavoidable, the address or previously saved bookmarks should be entered manually.

Morning Session – Panel II **Industry and Critical Infrastructure Vulnerabilities**

Aidyn Abjanbekov, General Director of Ericsson Kazakhstan served as Moderator of the Second Panel and spoke about *Being Secure in the Transition to 5G*. As Ericsson is on the cutting edge of 5G development, Mr. Abjanbekov opened the Second Panel with a description of 5G telecommunications technology. With the advent of 5G and its introduction in certain countries, these new networks must be prepared to combat new threats. The presentation outlined Ericsson's approach to its in-house network and Cloud Security measures, introducing its *RAN Security* solution for the Ericsson radio network, and the *Cloud Core Security* solution, which protects Cloud storage through various perimeter defense measures.

Andrey Kurilin, CEO of Citibank, addressed *Cyber Trends and Resilience* – a crucial topic for one of the largest international banks. He began by outlining trends that lead to new risks such as digitalization, government regulations, mergers and acquisitions, and the obsolescence of traditional cyberthreat assessment methods.

On *digitalization*, the use of new technologies often overlooks the need to secure them from threats. On *government regulations*, laws that concern privacy, data localization, employment, and outsourcing at times conflict, thus compromising a company's ability to respond quickly. On *mergers and acquisitions*, different companies may use incompatible operating systems, so “bridging this gap” can leave the new company vulnerable while it integrates systems and operations. Finally, on the *obsolescence of assessment methods*, modern data-dependent companies need to devise new measures to evaluate risks and assets into quantitative measures to distribute the necessary resources into cybersecurity measures.

All levels of a company are responsible for its security, which can be summarized as the three stages of a crisis: *prevention*, *exposure*, and *reaction*. Across these areas, it is important to coordinate the people, processes, and technologies responsible for defense, crisis management, and reaction to strengthen the company as a whole.

Kaspars Kukelis, CEO of Kcell, addressed *Cybersecurity for the Telecommunications Industry*. Mr. Kukelis noted that Kazakhstan faces three main threats in this field. *First*, the population has yet to understand the value of digital information and its security. *Second*, overly complex authentication systems inhibit quick responses to cyberattacks. *Third*, the telecommunications monopoly is now giving way to a multitude of service providers, which complicates responsibilities and types of effective security measures.

Kcell knows cyberthreats since it was the target of an attack in 2013 to steal subscriber funds. With this in mind, he stressed the importance of protecting networks in the face of constantly evolving technologies such as 5G. New technologies can bring about new benefits, but they also introduce new vulnerabilities in their integration.

Ivo Aalbers, General Manager of IMT/IT for the North Caspian Operating Company (NCOC) addressed the critical topic of *Cybersecurity for the Oil & Gas Industry*. He outlined the necessity for the energy industry to use new technologies and increased automation, but this push for innovation must be matched with preparedness to face the complexities of their integration with older systems and processes.

As a critical sector in Kazakhstan's economy, the oil industry is a target for both state and non-state actors. Attacks on the oil and gas industry have significant knock-on effects down the value chain in energy production, usage, and consumption. To meet this challenge, a *Cybersecurity Culture* must be created in which employees at all levels are aware of the appropriate measures to protect themselves and the company from cyberattacks. This will limit the types of attack vectors that a malicious actor could leverage.

Ruslan Stefanov, Lead Consultant of Industrial Cybersecurity at Honeywell, spoke about *Cybersecurity for the Oil and Gas Industry*. With a background in providing cybersecurity solutions for this critical industry, his presentation showcased Honeywell's new *Forge Cybersecurity Platform*. This is a solution that augments *Operations Technology* teams. These services simplify OT cybersecurity management, strengthen company-wide cybersecurity measures, and, with three types of services (site, enterprise core, and enterprise premium), are scalable to allow a variety of organizations to benefit from its services. These services will also help companies save time, comply with security regulations, decrease response times to attacks, and save money.

Afternoon Session – Panel III ***Protecting Government, Industry, and the Individual***

Piotr Marczuk, Corporate Director for Microsoft Central and Eastern Europe, delivered recommendations for *Creating a Healthy and Safe Digital Ecosystem for the Future*. He began by focusing on the worrying trend that an increasing number of cyberattacks are state-sponsored and that the damage done increases with every year. With that, he outlined Microsoft's security posture through protection, detection, and response. He also introduced the development of Microsoft's ethical and effective AI to augment existing cybersecurity measures and develop new measures.

Lastly, in response to modern Cyberthreats, Microsoft showcased two of its services. *First*, its *Digital Crimes Unit (DCU)*, which works closely with Europol and Interpol to assist in capturing cybercriminals leveraging Microsoft's resources and advanced data analytics. *Second*, its *Government Security Program (GSP)*, which augments a government's Cybersecurity measures to protect it from unscrupulous state and non-state actors. Together, these services create more accountability, defend sensitive systems, and promote the rule of law in cyberspace.

Andrey Gusakov, Director of Security and Industrial Solutions at Oracle Russia outlined *Oracle's Contribution to Cybersecurity for Business, Public Services, and Individuals*. His presentation showcased innovative Cyberdefense capabilities through automated, intelligent security systems, which segued to his introduction of Oracle's *Management Cloud (OMC)* and its *Orchestration Cloud*. As these are autonomous, they can increase authentication measures upon threat detection.

The Orchestration Cloud has an additional feature in that it can actively patch itself "on the fly." These innovations will undoubtedly be integral in the future of security systems. He also introduced the *Oracle Database Security Assessment Tool (DBSAT)*, which identifies

system vulnerabilities and makes recommendations. This allows users of this service to quickly comply with a variety of data security regulations around the world, building an organization's resilience while making it legally compliant.

Vladimir Remyga, Risk Advisory Director at Deloitte Kazakhstan, focused on *Cyber Crisis Management: Readiness, Response, and Recovery*. This topic focused on analyzing the aftermath of attacks to better prepare for future ones, and drew an analogy between cybercrimes and physical crimes where IT teams should "preserve the crime scene" rather than "cleaning it" to return to normal operations.

Although preserving the compromised systems can create a vulnerability to future attacks, on the other hand, returning to normal operations limits the short-term financial loss that a company may incur from an attack. In either case the end of the crisis does not mark the end of the crisis response cycle. There are many steps that a company must take to protect itself, such as rebuilding stakeholder confidence, analyzing data from the attack, and developing its security posture to create greater strength in the future.

Mikhail Betin, Kazakhstan Director of OSG Records Management, spoke about *Protecting Confidential Documents and Records Against Cyber Threats*. He outlined methods used by OSG Records Management to protect confidential information in its paper and electronic archives. With the advent of advanced forms of computer hacking, protecting information requires a secure physical database – it must be fireproof, earthquake resistant, and employ 24-hour security measures.

Older methods of information security keeps archives and documentation safe from modern threats that aren't designed to deal with physical vaults and security guards. On the other hand, having an electronic archive is a necessity as the modern mobile and flexible work environment require a more flexible means of information storage and extraction. OSG provides both to create a balance between physical security and secure global access.

Kurmangazy Talzhanov, a Partner at Integrites Law Firm, delivered his presentation on *How to Curb a 'Trojan Horse.'* Mr. Talzhanov focused on recommendations for companies to both avoid Cyberattack risks and remain compliant with Kazakhstan's Cybersecurity legislation. He recommends companies apply due diligence to find weaknesses within their anti-virus systems; form rigorous internal policies on the management and storage of confidential data; develop their in-house IT and legal teams to better protect the company on these fronts; and adopt *CyberHygiene* through IT workshops so that everyone within the company is aware of the dangers posed by malicious actors who target the least aware or least experienced in an organization.

Afternoon Session – Panel IV

Digitalization and The Cloud: Benefits and Risks

Ashley Clarke, Chief Operating Officer of KPMG Kazakhstan, moderated the Conference's final panel with a few remarks about Cloud development. The Cloud and its services are becoming increasingly integrated into business functions, and KPMG's work in this field shows this is the current trend amongst businesses of all types.

Konstantin Aushev, KPMG's Cybersecurity Director, continued this theme with *Cloud Governance and Security*. Interestingly, in the face of data privacy concerns, the usage of CRM (*Customer Relationship Management Cloud*) services has only increased. Cloud architecture now covers all key aspects of IT management, ranging from services to utilities.

While this new environment entails new potential threats, KPMG recommends companies aiming to invest in Cloud infrastructure to scale their needs to their capacities; match usage to an appropriate storage class; pick an appropriate pricing model; and continually monitor usage to ensure total cost of ownership is within acceptable parameters. Companies can then invest in Cloud services safely and prudently.

Vitaly Sokolov, a Partner at PwC Russia, delivered the Conference's final presentation, *Digital Trust Insights*. These insights constitute a list of recommendations stemming from conclusions on survey data from PwC's *Global State of Information Security Survey (GSISS)*. Mr. Sokolov showed how these insights revealed incongruencies between Cybersecurity policies, concerns, and practices.



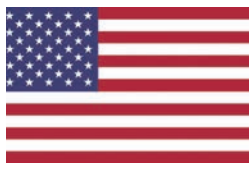
He recommended that companies engage with security experts at the start of digital transformations; improve communications between IT specialists and the board of directors; boost a company's Cyber-resilience; be proactive in legal compliance; and, lastly, keep pace with innovation. These recommendations were further distilled into discreet, actionable policy prescriptions ranging from adjusting corporate management structure to investing in academic research on Cybersecurity topics.



Final Remarks

Common threads united the expert speakers from many industry and non-industry sectors at the Conference:

- *First*, creating a more secure digital environment is a community effort. Sharing knowledge and strategies provides a greater immunity internationally, country-wide, organizationally, and for the individual.
- *Second*, ensuring cybersecurity is a responsibility across all levels of an organizational structure. No longer can these issues be relegated to IT professionals alone. All staff must learn basic Cybersecurity Hygiene—the chain is only strong as its weakest link
- *Third*, as states and companies enter the purview of Cyberspace, all organizations will need to invest in their security teams and safer procurement practices. Cybersecurity needs to be treated as an integral aspect of an organization's functions. Executives need to revalue the importance of their digital information and ensure that IT and OT teams have the appropriate resources and funding to protect it.
- *Fourth*, the usage of pirated, unlicensed/under-licensed programs and operating systems, with their built-in threats and vulnerabilities must be re-evaluated and eliminated. Their usage is not only a legal issue, but an invitation to cyberattacks.
- *Fifth*, an incident is only the beginning. Understanding the nature of attacks after the fact – the vectors, targets, motives, and tools – is integral to improving an organization's security posture.
- *Last, but not least*, as Kazakhstan's economic and geopolitical power increase, both the country and the companies that operate within the country, will become a more attractive target for Cyberattacks. The development of *Digital Kazakhstan's Cybershield* will be crucial, but Kazakhstan is not alone in this endeavor. It's allies, ranging from local firms to multinational companies and diplomatic supporters, stand ready to lend advice and assistance.



WHY CYBERSECURITY MATTERS

KEYNOTE SPEECH BY WILLIAM MOSER,
U.S. AMBASSADOR TO KAZAKHSTAN

Networked technologies touch every corner of the globe and every facet of human life. They have driven innovation, nurtured freedoms, and spurred economic prosperity. Even so, the very technologies that create these opportunities are exploited by cybercriminals, both state-sponsored and financially driven hackers, that target networks and threaten to weaken State institutions. Vulnerabilities and threats from data breaches, denial of service attacks, malware, ransomware, and “cryptojacking” – a sample of the types of threats – grow exponentially each year. Last year, breaches like these impacted more than 60 million Americans, which, at times, led to devastating personal and commercial financial losses.

That is why, each October, the United States recognizes *National Cybersecurity Awareness Month*, a collaborative effort between the government and industries to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online. As part of last year's Cybersecurity Awareness activities, the U.S. Mission to Kazakhstan organized a cybersecurity symposium in partnership with the Nazarbayev University, which featured cybercrime experts from the U.S. Federal Bureau of Investigation (FBI).



At the symposium, FBI agents brought to light the explosion of global identity theft stemming from embedded “backdoors” in software, such as trojans and malware. They also elaborated on how identity theft is directly related to all forms of intellectual property theft and trafficking in counterfeit goods. Increasingly, criminal groups are using malware and bots to collect personal information and “daisy chain” millions of computers to conduct other criminal activities such as virtual currency mining and money laundering. Malware and bots also pose national security threats to countries that fail to restrict the use of pirated and under-licensed business software.

The use of under-licensed software threatens critical infrastructure and government agencies as well as the financial livelihoods of businesses and the privacy of consumers' data. The United States welcomes Kazakhstan's initiative to develop a comprehensive cybersecurity policy through the *Cybershield* and *Digital Kazakhstan* projects.

Ensuring data integrity, protecting critical infrastructure, and enforcing the rights of inventors and creators is vital not only to our shared security but also to our shared prosperity. In the United States, the private sector and civil society play key roles in that process, so the public sector, the private sector, and society as a whole need to find new ways to collaborate on policy responses to deal with the cyber-threats that menace them.



U.S. Ambassador William Moser

President Nazarbayev set an ambitious goal of transforming Kazakhstan into one of the world's top-30 economies by 2050. To realize this goal, a conducive and supportive policy framework is critical. The government will not only need to protect its companies and citizens from cyberattacks and data theft, but also create an enabling environment for businesses to develop innovative solutions to cyber-challenges. This endeavor would include developing a robust framework for protecting intellectual property rights.

In the *US's National Cybersecurity Strategy* released last year, President Trump committed to ensuring the security of cyberspace and to working with allies to promote a secure and thriving digital economy. In support of these efforts, the United States launched a program called *STOP. THINK. CONNECT.*, which provides an entire cyber-hygiene toolkit free of charge to U.S. institutions and international partners – many already translated into Russian. Led by the Department of Homeland Security's *Cyber Awareness Coalition*, this program is a public awareness campaign aimed at educating everyone about cyber-threats posed by networked technologies and empowering the public to be safer and more secure online.

As always, the US encourages its international partners, including Kazakhstan, to join the *Cyber Awareness Coalition*. Furthermore, the US government will continue to encourage dialogue between the public and private sectors on cybersecurity, as with the American Chamber of Commerce's Conference on Cybersecurity in Nur-Sultan, so that everyone will be able to enjoy the benefits of a secure, open, and innovative cyberspace.

THE CANADIAN GOVERNMENT APPROACH TO CYBERSECURITY AND PROTECTION OF PRIVACY

KEYNOTE SPEECH BY NICHOLAS BROUSSEAU,
CANADIAN AMBASSADOR TO KAZAKHSTAN



Canadian Ambassador Nicholas Brousseau

As malicious cyber tools are increasingly accessible and as rates of cybercrime continue to rise, cybersecurity has become essential to every country's economic well-being. In 2018, Canada had the third most cyber incidents, behind only the US and UK. In combatting these threats, Canada is also the fourth largest cybersecurity innovation hub.

As critical infrastructure is increasingly remote-controlled and as essential services are managed online, cyber incidents have the potential to compromise both national security and public safety. For example, nowadays, cars are as much computer as they are machine, and BlackBerry, a Canadian information technology company, now protects more than 150 million cars worldwide with its QNX software. Protecting cars against cyberattacks is directly relevant to public safety and security. Cybersecurity is now a fundamental element of automotive production.

Cyber incidents can be profoundly destabilizing. They can erode the people's trust in both electronic commerce and government institutions. Frustratingly, as innovation brings new technologies, it also changes the nature of cyberthreats, and governments need to be aware of them as these attacks can have a significant impact on both jobs and industries. This article will center on two themes: first, an overview of how the Canadian Government approaches cybersecurity and secondly, the intersection of cybersecurity and protection of privacy and intellectual property.

The role of combatting cyberthreats falls to many actors, but, in Canada, the government plays a leading role. For several years, the Government of Canada has conducted *National Cyber Security Threat Assessments*, with an unclassified version released to the public for the first time in 2018. These comprehensive reviews take a hard look at Canada's own systems and help understand what needs to be improved. In 2018, for example, the *Canadian Center for Cyber Security* (the government agency responsible for these reviews) concluded that:

- Cybercrime is evolving as cybercriminals take advantage of growing online markets for illicit goods and services. They are opportunistic in target acquisition.
- Cyberthreats are increasingly focused on stealing large amounts of personal and commercial data, which is used for theft and resale, fraud, extortion, or espionage.
- Canadians are very likely to encounter malicious online influence activity in 2019. It is anticipated that state-sponsored cyberthreat actors will continue to target Canadians' opinions.
- State-sponsored cyberthreat actors will also continue to conduct espionage against Canadian businesses and critical infrastructure.
- Sophisticated cyberthreat actors will likely continue to exploit the trusted relationships between businesses, suppliers, and service providers for espionage and other criminal purposes.
- Lastly, cyberthreat actors are adopting more advanced methods, such as compromising hardware and software supply chains, making detection and attribution more difficult than before.



To combat these threats, Canada created its *National Cyber Security Strategy*. The primary goals of this strategy are to protect the safety and security of Canadians and Canada's critical infrastructure; to promote and protect rights and freedoms online; and to encourage cybersecurity for businesses, economic growth, and prosperity. In the Canadian approach, the responsibility for cybersecurity and enacting the *National Cyber Security Strategy* does not fall to one department.

Fifteen individual Government Ministries and Agencies are involved in key roles that correspond to their expertise. Working together, they collaborate by securing Government systems; partnering with the private sector and civil society to secure vital systems and infrastructure outside the federal government; and helping Canadians be secure online.

Concerning the protection of privacy and personal information, there is obviously an overlap between protecting a country and its citizens from cybersecurity threats and protecting a citizen's personal information and privacy rights. In many cases, there is a natural synergy that stems from the fact that it is often precisely this information that cyberattacks target. However, it was found that a key weakness in the system, one that leaves everybody vulnerable, is the way that businesses and governments look at their responsibility towards protection of this vital information.

Too often, however, companies see necessary investments into cybersecurity as something that costs them money – a cost center – rather than a vital piece of the corporate infrastructure that keeps them operating. Canadian cybersecurity companies communicate that they specifically look for high-profile cybersecurity incidents as a part of their sales strategy because when a business or government in a particular community is hit by a cyberattack, everybody influenced by these tragedies begins to understand the consequences of being unprotected.



The Canadian solution has been to pass the *Personal Information Protection and Electronic Documents Act*, which obliges organizations (both private sector and government) to obtain an individual's consent when their personal information is collected, used, or disclosed. This Act ensures that people have the right to access their personal information held by an organization and that they have the right to challenge its accuracy. Under the Act, personal information can only be used for the expressed purposes for which it was collected. If an organization is going to use it for another purpose, it must obtain that individual's consent.

Furthermore, the Act obliges organizations to ensure that individuals' information will be protected by appropriate safeguards. The type of information covered by the Act includes a person's age, name, ID numbers, income, ethnic origin, blood type, opinions, evaluations, comments, social status, disciplinary actions, employee files, credit records, loan records, medical records, existing disputes between a consumer and a merchant, and intentions (for example, to acquire goods or services, or change jobs). Failure to protect this information or to disclose data breaches can result in fines of up to \$100,000, audits, or referrals to the Department of Justice for potential criminal charges.



These issues are challenging but vitally important. In many ways, governments, policymakers, and corporations are all "in the same boat" and grappling with the same challenges. The Canadian Government commends Kazakhstan for the steps it has already taken to address its cybersecurity challenges through the creation of its *Cybershield* as part of *Digital Kazakhstan*, and the establishment of a national cybersecurity strategy. Canada is always ready to assist Kazakhstan to address this global challenge, and innovative Canadian solutions are ready to be deployed in the country.



STATE-OF-ART CYBERSECURITY

SPEECH BY ANDRÉ CARSTENS, AMBASSADOR OF THE NETHERLANDS TO KAZAKHSTAN



Digital transformation has reshaped the world, and it will continue to disrupt the status quo. While technology is a key driver for realizing societal and economic benefits, it also brings about new security challenges. Governments, businesses, and civil society alike face a wide range of existing and emerging cyber threats.

- Firstly, there is the threat of disruption and sabotage – which would have severe impact on the national security of the Netherlands because of its potential for disruption to society.
- Secondly, there is the threat of Information and Communications Technology (ICT) operations by state and non-state actors for coercive political and military purposes. Sadly, cybercrime qualifies as a growth industry, and it increasingly threatens the security of states, stability in cyberspace, and international peace and security.
- Thirdly, there are ICT activities that aim to disrupt critical infrastructure including the integrity of democratic governance, the integrity of core internet functions, and the economic stability of societies.
- Lastly, there are aggressive and coercive ICT operations below the threshold of armed conflict. These types of strikes constitute the most urgent challenge to international peace and security. To this end, states must also be aware of the nexus between cybercrime and terrorism.

The resilience of critical infrastructure – although everyone knows that it is crucial for citizens, companies, and the government – consistently lags behind the growth and development of threats against it. Organizations are sometimes not prepared and are successfully attacked through simple methods. The necessary measures are not always taken due to the lack of a clear perspective on the costs and the benefits of effective cybersecurity measures. This complexity undermines the resilience of all organizations, and this lack of resilience carries forward, being detrimental to international stability. Addressing these deficiencies is a priority.

Governments and organizations alike need to highlight new and underexposed issues that warrant further attention; investigate and take the necessary actions in order to protect all societies from disruptions stemming from malicious actors in cyberspace; and ensure that vital societal infrastructure remains safe. Sharing best practices and expertise is a necessary step to secure critical infrastructure. Therefore, the government must develop trust and long-term commitments by sharing information across government agencies and between relevant private actors.

Ever since The Netherlands hosted the *Global Conference on Cyberspace* in 2015, it has played a leading role in spreading this message worldwide. The Netherlands operationalized this vision through developing its *National Cyber Security Strategy (NCSS)* and a baseline for enhancing its *Critical Infrastructure Resilience*.

Meanwhile, the Global Conference has already proven its significance by engaging 79 members and 19 partners, thus strengthening the ecosystem for international cooperation on cyber-capacity through the development of online tools for the best practices on *Critical Information Infrastructure Protection (CIIP)*.

This Global Conference continues to create tangible benefits. Governments now realize that CIIP is a matter of national security and therefore embed it within their state's national security strategy. The Global Conference also served to develop a clear terminology, which is crucial for understanding CIIP policy and for clear and coherent dialogues on this topic. The international dialogue for these policies also helps states keep track of changes by understanding new threats, creating measures to mitigate them, and identifying one's own vulnerabilities.



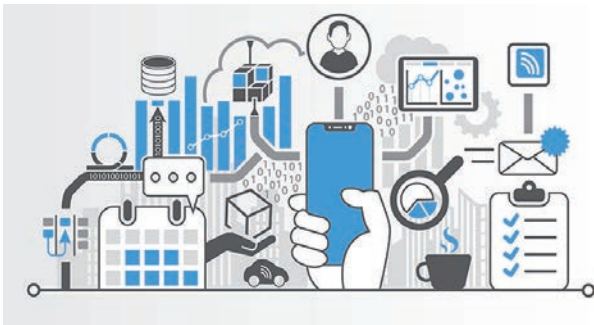
Finally, as The Netherlands is a maritime nation, the maritime sector is of specific concern. This industry is now digitalized along with the country's critical maritime infrastructure – ports, dams, dikes, and floodgates (crucial to protect the country from the sea). As they are digitalized, all of these systems can be remotely controlled, which constitutes a great threat to national security if these systems become compromised.

Internationally, the maritime sector is critical to trade and transportation for all nations. International cooperation is vital to secure the maritime sector and promote economic opportunity, as the impacts of an attack are not limited to one country. Cyberattacks on this critical sector will have knock-on effects in other countries and in other sectors. Therefore, all countries should continue to raise awareness, foster dialogue, and cooperate to manage the risks of living in a digital society.



KAZAKHSTAN'S DIGITALIZATION AND INNOVATION STRATEGY AND THE CHALLENGE OF CYBERSECURITY

KEYNOTE SPEECH BY ASKAR ZHUMAGALIYEV, MINISTER OF DIGITALIZATION AND INNOVATION OF KAZAKHSTAN



The Government of Kazakhstan is greatly invested in the future of e-governance, the economic benefits of digitalization and fostering market innovations, and cybersecurity. It is with this in mind that President Nazarbayev supported developing the *Digital Kazakhstan* program.

One of the main purposes of *Digital Kazakhstan* is to “create an ecosystem that promotes innovation.” This means that the Government will help foster conditions for the development of technological innovation and entrepreneurship by linking business, sciences, and the Government. The Government acts as a catalyst for the ecosystem as it is capable of generating, adapting, and introducing innovations.

From hacking social media profiles to the large-scale data theft, cyberattacks come in a variety of vectors and intents. The Digitalization Ministry is currently working to introduce Kazakhstan's *Cybershield* concept, which aims to ensure the safe use of information and communication technologies. Kazakhstan's *Cybershield* is a symbiosis of many cybersecurity strategies already applied in countries such as Estonia, France, Germany, and Norway.

Digitalization efforts worldwide and in Kazakhstan will create a new society where human capital is actively developing: knowledge and skills for the future are learned from a young age; business efficiency and speed are augmented through automation and other new technologies; and the interaction of citizens with their governments becomes simpler and more open. The digital revolution is happening before our eyes, and Kazakhstan will harness it and the rise the meet the challenges that lie ahead.

Today, the digital economy is growing at a rate of up to 25% per year in developing countries. No other sector of the economy can even come close to this pace of development. With the advent of this new sphere of the economy and the state, the Government and corporations spend nearly half a trillion US dollars annually to counter a new, wide-spread phenomenon – cyberattacks.

KAZAKHSTAN SEEKS TO PROTECT CYBERSECURITY- THE ROLE OF THE MINISTRY OF JUSTICE

KEYNOTE SPEECH BY MARAT BEKETAYEV, MINISTER OF JUSTICE OF KAZAKHSTAN

The active introduction of digital technologies and their integration into the global information sphere determines the success of any government. Digital platforms and electronic documentation ensure the transparency and efficiency of government authorities, businesses, public organizations, and, lastly, social and educational institutions.

Government electronic services provided through an online portal (e-governance) will improve the quality of life for all of Kazakhstan's citizens. With the advent of e-governance, however, there are also potential risks, threats, and challenges in the digital sphere associated with the use of information technology.

The American Chamber of Commerce's Forum is a great opportunity to share and discuss the most pressing issues of cybersecurity and cyber-crime. It is important that government representatives, leading companies, and cybersecurity experts share intelligence, advice, and concerns that may arise in the future with each other. The Kazakhstan Government position is that ensuring cybersecurity within the context of globalization and digitalization is the responsibility of the Government.

The Ministry of Justice is one of the leading executive authorities working with government databases, and it is actively participating in the process of digital integration. This Ministry is also tasked with implementing government policy for the protection and enforcement of intellectual property rights.

In its responsibility to secure cyberspace for the citizens of Kazakhstan, the Ministry of Justice, as well as the rest of the country's government, is ready for open dialogue. Confronting cybercrime at the state level should be done through the joint efforts of stakeholders: all Government authorities, business communities, public organizations, and the general population, whose needs cannot be ignored. Through this exchange of ideas, the Government and the private sector together can be better prepared to develop new integrated solutions and common approaches in countering the digital threats of today and tomorrow.



by **Andrei Yorsh**
Partner, Baker McKenzie

Software has become one of the main elements of the modern economy. One can hardly conceive the operation of any sector – energy, health, banking, communications, commercial, or defense – without the usage of software. The introduction of software tools increases competitiveness through automation of processes, cost reduction, and minimizing negative human factors. The deep penetration of software in all sectors of the economy, however, increases the need for its protection against the malicious actions of third parties.

According to research carried out by Juniper Research, cybercrimes accounted for approximately three trillion dollars in losses worldwide in 2018. Cyberattacks occur every 14 seconds, and, every day, darknet shadow markets receive text data from approximately 686,000 compromised payment cards.

Various methods are used to gain unauthorized access to databases and management software. These methods include exploiting vulnerabilities in computer programs and BIOS / UEFI, phishing, vishing, and viruses.

The problem of unauthorized access through system vulnerabilities within computer programs often stems from the usage of counterfeit software by government agencies and private companies alike. The use of counterfeit software by users, including those in Kazakhstan, is rationalized through the short-term cost savings of avoiding licensing fees and the 'high cost' of paying for software.

Such apparent savings result in huge financial losses for users. Since these users do not have the support of software manufacturers, they themselves provide hackers with access to their internal processes and databases due to inherent software vulnerabilities. Furthermore, such users are liable for copyright infringement. In Kazakhstan, such a violation entails criminal liability.

The most effective approach to combat cybercrime associated with vulnerable software is to use licensed software. Users who obtain the necessary support from manufacturers considerably reduce the risk of financial losses caused by cyberattacks. In addition, the risk of liability for infringing intellectual property rights is reduced to virtually zero.

Despite these self-evident truths, according to some experts 74% of software in Kazakhstan is counterfeit. As far as companies and individual users are concerned, they operate at their own risk. However, for government organizations and national companies, the problem is largely associated with legal loopholes. Neither the *State Procurement Law* nor the *Samruk-Kazyna Procurement Regulations* protect intellectual property rights. The only document that regulates these issues somewhat is the *Rules for the Procurement of Medicines and Medical Products* within Kazakhstan's statutory free healthcare program.

Kazakhstan has set itself the ambitious task of becoming one of the fifty most competitive countries in the world. Protection of intellectual property rights is one of the main conditions for achieving this goal in an innovative economy. Moreover, this is one of the most effective approaches to combat cybercrime and prevent the damage it can cause. The Government of Kazakhstan faces a serious challenge to address this issue in the near future.

Baker McKenzie.

LEGAL ADVICE Above Your Expectations

For the ninth consecutive year, Acritas has named our Firm the World's strong law firm brand, ranking us No. 1 globally in awareness, favorability, and consideration for cross-border deals and litigation.

bakermckenzie.com

Argentina | Australia | Austria | Bahrain | Belgium | Brazil | Canada | Chile | China | Colombia | Czech Republic | Egypt | France | Germany | Hungary | Indonesia | Italy | Japan | Kazakhstan | Korea | Luxembourg | Malaysia | Mexico | Morocco | Myanmar | Netherlands | Peru | Philippines | Poland | Qatar | Russia | Saudi Arabia | Singapore | South Africa | Spain | Sweden | Switzerland | Taiwan | Thailand | Turkey | Ukraine | UAE | UK | USA | Venezuela | Vietnam

Almaty

Samal Towers
97 Zholdasbekov Street
Almaty 050051 Kazakhstan
Tel: +7 727 330 05 00
Fax: +7 727 258 40 00
almaty@bakermckenzie.com

CREATING A HEALTHY AND SAFE DIGITAL ECOSYSTEM FOR THE FUTURE

by Piotr Marczuk
Government Affairs Manager, Microsoft

In today's digital world, technology is integrated into everything we do, and it is Microsoft's mission to empower everyone and every organization with technology to achieve more. With this in mind, there are nonetheless concerns that relate to all IT companies in Kazakhstan. The following article will not only outline these issues, but also submit some proposals for the benefit of a healthy digital ecosystem in Kazakhstan for the people, the government, and the investment climate.

There is a global trend today towards cloud computing and artificial intelligence. Cloud and AI are spreading around the world and becoming the key vehicles of economic growth. Companies, startups, and governments that adopt them are more competitive and grow their economies. There is a great opportunity that these two trends can be manifested in the Government of Kazakhstan's *Digital Kazakhstan* initiative with the help of its young, innovative society, but there are also policy obstacles that hinder its development.

With the growing digitalization of countries and societies, there is a dangerous increase in cybercrime. Companies, citizens, and governments are all victims of cyberattacks, losing trillions of dollars in stolen intellectual property (IP), money, and through reputational damage. Microsoft has worked for years to help track down cybercriminals through its *Digital Crimes Unit (DCU)*, which assists Interpol and Europol in bringing these criminals to justice through its specialized teams and advanced data analytics.

Microsoft's DCU services include tech support fraud, online child exploitation, global strategic enforcement, cloud crime and malware, and defense against Nation-State Actors. It is evident that cybercrime is a complex issue and a global problem, and while post-crime investigations are crucial, the best defense is to increase a system's resilience against attacks to protect all users within a country.

Another worrying trend that Microsoft's analyses track is an increase in sophisticated state-sponsored cyberattacks. These so-called *Advanced Persistent Threats (APT)* are extremely dangerous. We see approximately 30 countries in the world that have cyber-offensive capabilities with the potential to impact entire economies or strike critical infrastructure. For example, the *WannaCry attack*, attributed to North Korea, took down the UK's National Health Service by using malware to exploit unpatched software. These are the key risks that the Government of Kazakhstan should consider and for which it should be prepared.

Looking into the last threat intelligence report published by Microsoft in 2017, there is a worrisome trend in Kazakhstan – an extremely high level of malware on devices used in the

country. It's considerably higher than the world average or the average for European countries. This malware problem has knock-on effects as global companies take into account cybersecurity risks when making investment decisions. A dangerously high incidence of malware may actively decrease foreign investor confidence in Kazakhstan, and this is even before considering how local enterprises are affected when their computers are frozen by ransomware, thus drastically decreasing productivity.

Concerning Digital Kazakhstan's objectives, Microsoft outlines three key principles slowing digital development:

- *the cybersecurity risks mentioned above;*
- *a lack of clarity or misinterpretation of personal data protection regulations, leading to a reluctance by a Government agency or institution to use cloud technology for public sector solutions;*
- *data localization policy as stipulated in the Law on Informatization.*

To advance Digital Kazakhstan and address cybersecurity concerns, Microsoft recommends the following:

- *Strengthen collaboration between Government and the IT Industry to improve cybersecurity through basic "hygiene" and an awareness of modern cybersecurity threats;*
- *Eliminate the usage of unlicensed software;*
- *Create a working group composed of the Government, business, and the IT Industry to identify and amend data management policies and to build upon the best practices from the EU and other countries.*
- *Develop through the Government official cloud computing guidelines with appropriate security safeguards to accelerate the Digital Kazakhstan program and AI development within the country.*

Microsoft designed the *Government Security Program (GSP)* to intensify cooperation with governments. It provides governments with the confidential security information and resources they need to protect themselves and their citizens against modern cyberthreats. GSP provides governments access to security information about Microsoft's products and services, data (on and offline) that improves protection of information technology against cyberthreats, and collaboration between Microsoft's teams with the government's cybersecurity experts.

Microsoft also envisions a future where Kazakhstan's law enforcement agencies collaborate closely with Microsoft's DCU to make its economy and society safer. Through Digital Kazakhstan, the country will be entering into an innovative, but dangerous new environment. However, with the help of the private sector, Kazakhstan can create a healthy digital ecosystem for the future.

Success starts with security

Security is the number one focus and priority for organizations today. Protecting your organization continues to be increasingly difficult as employees use their own devices and applications at work and data flows into and out of your business in a variety of ways. Big data is transforming how security experts defend against cyberattacks - and Microsoft is leading the way. Our global reach generates billions of data points that help us diagnose attacks, reverse engineer advanced threat techniques, and apply intelligence to strengthen your security.

Microsoft transforms worldwide security intelligence into products and insights that power and protect our customers' connections. Learn more about how the breadth and depth of our security works for you at microsoft.com/security.



CYBERSECURITY FOR THE OIL & GAS INDUSTRY

by Ivo Aalbers
General Manager IT & IM
North Caspian Operating Company (NCOC)

The oil and gas industry lies on one end of an integral, high-value supply chain, which ranges from exploration and extraction to refinement, power-production, and consumption. It's an age-old critical industry, but with the modernization and automation of extraction and production processes, the industry is a prime target of cyberattacks by both private and state-supported actors. This article will outline key areas of concern for the industry and NCOC's strategy to meet the challenge of cyber threats.

Going into the future, prosperity in the industry will be predicated on a company's ability to defend against, manage, and overcome cyberattacks. Increasingly, however, the types of attacks and their motivations vary greatly. *State-controlled attacks* against oil and gas systems serve to undermine or control production for strategic purposes. *Exploratory hacks* from private actors seek to obtain information about a company's operations. *Dissatisfied employees* may, themselves, seek retribution by damaging critical systems. *Industrial espionage* by other companies aim to seek an unfair advantage in the market. *Criminal actors* seek to conduct blackmail or ransomware attacks for monetary gain. Finally, *transient device hacks* can sneak malicious programming into a company's systems by accident by well-intentioned personnel through connection to secure systems that bypass firewalls.

As evident, the threat ecosystem is as diverse as the methods used to conduct attacks and addressing them has also been plagued with issues. Obsolete administrative splits between *Information Technology (IT)* and *Operations Technology (OT)* teams limits cohesion in their responsibilities and their ability to respond. Inconsistent cybersecurity standards, irregular patching, and the necessity to upgrade older control systems all further complicate the issue as well.

All of these threats and shortcomings to manage them are very real and extremely problematic for a highly targeting industry. Companies that fail to prepare for these types of scenarios will be vulnerable to them, which not only threatens the company but its personnel, its assets, and the wider public.

In response to these threats, NCOC is focused on the following cybersecurity concerns:

- *harm to people and the environment;*
- *harm to assets and facilities;*
- *a general lack of awareness or training on best practices;*
- *onshore and offshore facility connections, remote operations, outdated control systems; insufficient data-network separation;*
- *the usage of IT products with known vulnerabilities;*
- *insufficient physical security measures*

A crucial step is the development of a "*Cybersecurity Culture*." This means the creation of "*a positive cybersecurity culture that exists when a set of shared values and beliefs about Information and cybersecurity influences actions, and drives practices to preventing cybersecurity events*

Developing this culture and cultivating this awareness throughout all tiers of the company will decrease its vulnerability from threats that rely upon unwitting agents or breaches of security protocols. An extension of this is executive-level attention to cybersecurity measures. Executives need to view cybersecurity as a crucial aspect in the operations of an oil and gas company. They must work to attract skilled cybersecurity teams and executives in order to effectively manage this threat.

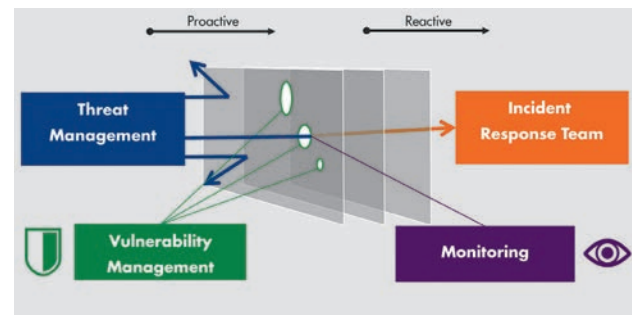


Figure 1 Bow-tie analysis and preparation

With regard to security strategies, NCOC adopted the industry standard "bow-tie" approach towards threat management, which can be visualized in Figure 1. By outlining the threats, vulnerabilities, and response and recovery capacities of NCOC, the company can prepare a multitude of strategies, policies, and response methods to counter all perceivable types of strike scenarios. In this manner, the company is proactive in preventing effective cyberattacks while preparing for incident management if an attack "slips through" defensive measures.

NCOC's success, and the prosperity of the industry as a whole, will rely upon maximizing the benefits derived from automation, IoT, and digitalization while managing the vulnerabilities created by using these very systems.

The North Caspian Project, the first major offshore oil and gas development program in Kazakhstan, is proving to be a great opportunity for Kazakhstan, the NCOC team, and local communities. As the effects of an attack threaten the greater communities at large that rely upon the success of this project, the NCOC team is devoted to developing strong cybersecurity measures to protect people, NCOC assets, and the environment.

CYBER CRISIS MANAGEMENT READINESS, RESPONSE, AND RECOVERY

by Vladimir Remyga

Director, Risk Advisory, Deloitte Kazakhstan

Hacked devices, crashed websites, breached networks, denials of service, copied emails, stolen credit card data – these are just a sample of the types of cybersecurity breaches that have become commonplace in our world. It's enough to leave one thinking that perhaps no organization can achieve absolute security in cyberspace. Most organizations develop some level of cyber incident response (CIR) capabilities, but those capabilities, which are often weighted toward short-term responses and IT issues, may fail to contain the effects of a cyberattack.

Avoiding such crises involves managing an incident before, during, and after it unfolds. This starts with evolution within cyber crisis management. For example, executives often see cyber incidents as “an IT issue,” but IT is only one domain. To ensure security, everyone must recognize that effective crisis planning involves multiple functions, domains, and skillsets. They also must be highly coordinated to effectively manage and contain an incident.

The Need for Crisis Planning

According to CBS, 1.5 million cyberattacks occur every year. This translates to over 4,000 attacks every day, 170 every hour, or nearly three every minute. While few attacks succeed, the high probability of cyber incidents dictates that every organization needs to be prepared. Effective preparation addresses the entire crisis management lifecycle: readiness, response, recovery (see Exhibit 1). Each phase of this lifecycle presents opportunities to protect the organization from risks, costs, and damage caused by an incident and strengthen the organization's defenses in the face of future attacks.

Readiness

Readiness is not only vigilance, such as 24/7 Monitoring, but also the readiness of resources. A well-prepared, multifunctional team must be poised to manage all aspects of a cyberattack. Also, crisis simulation and war-gaming enable management to understand potential threats, how to minimize risks, and whether or not the organization is truly prepared to handle real strikes.

Response

Management's response can either contain or escalate an incident – a poor response can even create a new crisis. Vigorous, coordinated responses to incidents limit lost time, money, customers, and damage to a company's reputation.

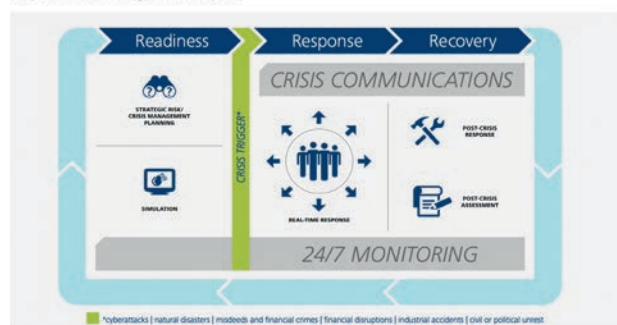
Management must be prepared to communicate across all media, including social media, to assure stakeholders that the organization's response can effectively meet the threat and overcome it.

Recovery

Measures to return to normal operations and limit the damage done to the organization and its stakeholders after an incident is crucial. Post-incident measures include assessing the cause(s), analyzing the company's crisis management capabilities, and eliminating deficiencies to better prepare for future strikes. Effective crisis management extends beyond preparing to manage specific events but rather to develop broad, flexible capabilities that enable a response to a wide range of events. The development of a secure, vigilant, and resilient organization will deter future instances.

IT and digital assets now drive a majority of an enterprise's value. With this in mind, attackers target organizations repeatedly and from various “angles” to capitalize on a system's vulnerabilities. Therefore, the risk that cyber crises pose to a company's reputation, its operations, and its customer-supplier relationships will continue to increase – as will the associated legal and financial effects. No board of directors or senior executive team can credibly deny the danger or likelihood of cyber threats. So, it is crucial to prepare a highly effective cyber crisis management plan before an attack occurs.

Exhibit 1
Deloitte's crisis management lifecycle



Being Secure, Vigilant, and Resilient

To better secure an organization in cyberspace, an organization should strive to become:

Secure

A secure organization prioritizes the value of its digital assets. All data is not created equal, nor is it practical or possible to provide complete security for all data. By prioritizing the value of digital assets, management can allocate resources towards them to obtain a level of security that corresponds to their value.

Vigilant

Vigilance demands that everyone be aware of how one could expose the organization to cyber risk through one's own devices, social media, and online conduct. A vigilant approach relies upon gathering intelligence and gauging the range of threats that could harm the organization. In addition, policy development, training, and accountability regarding cyber incidents each play a key role as well.

Resilient

A resilient organization aims to minimize the impact of an incident on its stakeholders while quickly restoring operations, credibility, and security. The rapid detection of cyber incidents combined with well-structured recovery plans can usually limit this damage, remediate the situation, reduce future risk, and then allow the organization to return to normal operations.

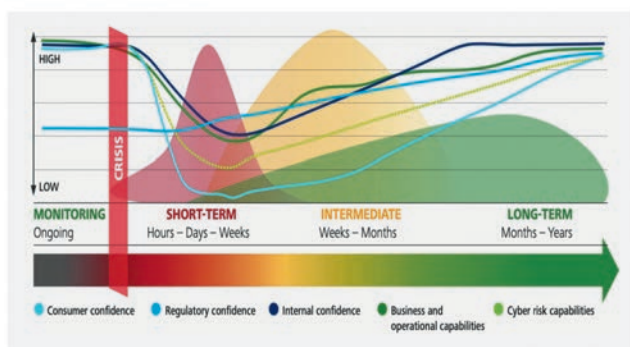
A secure, vigilant, resilient organization has all three phases of management, and Deloitte strives to achieve this ideal state as an organization and render its services to enable its clients to do the same.

The Cyber Incident Response (CIR) Lifecycle

While the precise nature, location, and impact of incidents cannot be predicted, the incident response lifecycle follows a predictable path (see *Exhibit 2*). Containing an incident and avoiding a crisis calls for a proactive approach in addressing stakeholder concerns.

Customers, for example, express concern regarding the loss of personal data and privacy and may develop a long-term brand aversion. *Business partners* are concerned about short-term cross-contamination of their systems and long-term integrity of data and transactions while employees may be overwhelmed by negative publicity and increased stress. *Regulators* want assurances regarding consumer protection and the state of the industry as a whole. Lastly, *Investors* are attuned to both the short-term financial impacts and long-term business/brand viability.

Exhibit 2
Cyber incident response lifecycle



The CIR lifecycle (*Exhibit 2*) illustrates the interplay between organizational capabilities and stakeholder confidence. Immediately after an incident, the affected capabilities must be restored – this usually takes hours or days but can take weeks or months in severe cases. Cybersecurity must also be enhanced to secure the environment, improve visibility into threats, and reduce the impact of future incidents.

Throughout the response lifecycle, crisis communication stands among the highest of priorities. Specifically, the organization must:

- Respond to a high volume of requests from customers, business partners, vendors, regulators, law enforcement, and the board of directors.
- Manage requests from business partners to modify arrangements, processes, and methods of sharing information.
- Engage in proactive messaging to the broader base of stakeholders and the public regarding what is known and not known about the cyberattack, and what the organization is doing in response to it.
- Monitor and address traditional web-based and social media reactions to the event and to the organization's response.

Additionally, management must:

- Address any potential threat of legal or regulatory action, and determine what legal recourse is available to the organization.
- Minimize the time between developing and implementing the remediation plan, while also managing the risks generated in that interim.

The more comprehensive and tested the plan, the better the management's response to an incident will be. Yet management should understand that the plan does not represent a script that will play out in reality and that responses must be flexible and fluid. You may have to depart from the plan, but the plan will provide a framework and guidance for coordinating the diverse elements involved in the response.

Getting Coordinated for Cyber Incidents Post-incident Investigation and Response

A digital crime scene is analogous to a physical crime scene – disturbing it can interfere with the work of forensic teams. Teams should start by securing the digital “crime scene” and preserving the evidence. Without an effective investigative

response, the causes of the incident may never be understood, and the risk of a recurrence may actually increase. Speed is essential for this process.

Sometimes, however, it is necessary to save the “victim” – a damaged or compromised system integral to the operations of a business. In these cases, that system cannot be simply secured and preserved but must be rescued and restored as quickly as possible. Businesses need to balance the decision to interfere and save the system with the need to preserve evidence for analysis.

To identify causes and remedies and hasten recovery following a cyber incident, a company should:

- Document how the incident was discovered, who reported it and how they were alerted. Interview IT staff and other relevant parties as a part of the investigation.
- Consider and research the possibility of insider involvement and take steps to minimize this risk going forward.
- Identify the affected systems and isolate them so that no one attempts to fix, patch, or alter the state of it.
- Gather all available evidence and analyze it to determine the cause, severity, and impact of the incident.
- Strengthen network security, improve protocols, and increase vigilance as indicated by the analysis.
- Enhance monitoring and other security measures to mitigate future risk from similar incidents.
- Document and report the findings to the relevant stakeholders and consider requirements to report incidents to a regulatory body.

To achieve this in practice, cyber-incident response programs require active coordination in six key areas: governance, strategy, technology, business operations, risk and compliance, and remediation (see Exhibit 3).

Governance

Governance frames the way a company organizes and manages its response team. It ensures intra-organizational coordination across functions (cross-functionality). Governance also aligns the response strategy with the company's goals and provides mechanisms to achieve it.

To establish governance for response management, a company must:

- Segregate duties by establishing an independent investigation team to help determine causes and remediation steps.
- Consider the role of legal counsel, who should be on or represented on the response team, which should be led by a business manager (to foster a cross-functional approach to CIR).
- Define the incident response and recovery lifecycle phases and establish a decision framework with clear action plans and measures of success.

Exhibit 3
Cross-functional capabilities required for effective response



Strategy

A response strategy defines how a company leads, prioritizes, and communicates during incident response and crisis management. Organizations should align the response strategy with the organization's responsibilities and values. A sound strategy frames a cost-effective, well-supported, organization-wide approach to addressing cyber incidents. This minimizes “tunnel vision” in response planning and reduces any adverse impact on operations and revenue.

To create an effective response strategy, a company must:

- Define escalation and prioritization processes to manage and coordinate IT, operational, and business recovery.
- Engage the organization's government affairs team or other government liaison to inform and work with regulatory agencies and relevant government officials.
- Align response efforts with security management and IT engineering initiatives.

Technology

The IT and cybersecurity teams develop and implement mechanisms for detecting, monitoring, responding to, and recovering from a cyber incident. IT engineers create the needed architecture, and then IT teamwork to maintain system resilience to attacks. Additionally, technical forensic and investigative capabilities are vital to preserving evidence and analyzing control failures, security lapses, and other conditions related to the incident. Organizations should implement both proactive and responsive technologies to mitigate and manage future cyber incidents.

To frame the technological aspects of incident response, companies must:

- *Be realistic about IT tools – they enable security and operational capabilities, but they do not eliminate risk.*
- *Resolve the tension between the immediate needs in the wake of an incident and long-term remedies*
- *Accept that “workarounds” and “throwaway work” are often necessary to meet short-term priorities*

Business Operations

After an incident, critical business operations must resume as soon as possible to minimize disruptions that have an impact on finances, reputation, regulation, and stakeholders.

To minimize business disruption, companies should:

- *Implement out-of-band processes to replace those that are broken or that present too many constraints on incident response or remediation.*
- *Plan for surge support and allocate resources accordingly.*
- *Understand existing business limitations such as the risks associated with using standard payments systems or applications.*

Risk and Compliance

Risk and compliance functions should assess and manage the regulatory compliance during incident and crisis response by interfacing with legal counsel, regulators and law enforcement.

SINCE

1865

Bertling



BERTLING – ALWAYS
A SMART MOVE



Bertling plans globally and performs locally. Freight forwarding projects are managed and executed to the highest technical standards. Bertling uses experienced, in-house personnel, robust group-wide systems, and puts together teams dedicated to your global business. For more than 150 years, Bertling's innovation has delivered operational excellence.

Your Freight Forwarding Specialist in Kazakhstan:

Bertling Kazakh Logistics LLP
Admiral Lev Vladimirsky Str.
Building #9
E02A4H5 Atyrau
Kazakhstan

Contact: Colin MacIsaac, Regional Director
Phone: +44 7585 902187

Contact: Aliya Zhaksylykova, General Director
Phone: +7 7122 763171

For example, after an incident, investigative processes and responses must be documented to demonstrate their adequacy. regulators, and law enforcement. For example, after an incident, investigative processes and responses must be documented to demonstrate their adequacy.

To successfully manage risk and compliance after an incident, a company should:

- *Anticipate requests from regulators and law enforcement, which may include requests for access to systems and a review of response activity.*
- *Analyze the impacts and loss exposures for insurance and other reporting purposes.*
- *Understand additional risks brought about by ad-hoc processes, technology, and workarounds required during incident response.*

Remediation

Remediation begins after critical business operations resume, with short and long-term efforts. The organization must verify that the attack vectors are eradicated and take steps to prevent similar attacks in the future. Remediation must also eliminate or minimize the root causes of incidents and return businesses to a secure operating environment.

To successfully remediate a cyber incident, a company must:

- *Balance the inclination to secure digital assets against the need to do business seamlessly.*
- *Prioritize the influx of technology project requests alongside increased IT budgetary requirements.*
- *Prepare for increased regulatory scrutiny and a potentially more rigorous regulatory regime*

The response team should include individuals from each of the previous six areas to develop a well-resourced, balanced, consistent approach to cyber incidents and cyber crises across the organization.



Conclusion

Deloitte's work in crisis management with senior executive teams yielded the following five lessons:

1. There's no substitute for preparedness.

Wargaming, rehearsals, and other structured preparations do much to position the organization to launch a coordinated response.

2. Every decision counts.

In a crisis, every decision can affect stakeholder value mainly through heightened reputational risks, which can destroy value faster than operational risks.

3. Response times should be in minutes.

Teams on the ground must respond rapidly, not in hours or days. They must take control, lead with flexibility, act on incomplete information, communicate well, and inspire confidence.

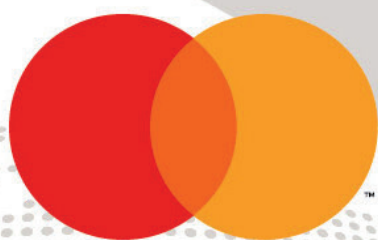
4. When the crisis has passed, work remains.

Even after breathing a sigh of relief, teams must capture data, log decisions, manage finances, handle insurance claims, and meet legal and regulatory requirements.

5. Companies can emerge stronger.

Almost every crisis creates opportunities for an organization to shine by responding effectively and seeking out opportunities to improve.

Customers, suppliers, employees, and other stakeholders understand that crises will occasionally affect the organization. What is not acceptable to them is a lack of preparation, inadequate responses, and confusing communications on the part of management. A part of the problem is that most organizations lack the resources to develop and maintain all the necessary incident and crisis response capabilities in-house. The expertise required, the evolving risk landscape, and the resources of cybercriminals render this impractical for most, and, while 24/7 monitoring can provide early warnings and risk sensing can detect patterns of criminal activity, these capabilities are not economically viable for most organizations.



mastercard.



Mastercard® is a technology company in the global payments industry.

Mastercard products and innovations enable to make purchases, travel, run business and manage finances in a simple, safe and effective way.

Mastercard makes its contribution to developing digital and cashless economy in Kazakhstan.

START SOMETHING PRICELESS WITH MASTERCARD

mastercard.kz

BEING SECURE IN THE TRANSITION TO 5G: ERICSSON'S APPROACH AND SOLUTIONS

by Aidyn Abjanbekov
General Director, Ericsson Kazakhstan

The 5G network will be the backbone of digitalized economies and societies around the world. It is a critical platform for commercial and societal transformation, which is why security is its essential component. Billions of connected objects and systems will be affected from critical sectors such as power generation and transmission, transportation, banking, health, and infrastructure (smart cities) to industrial control systems (which carries sensitive information and supports other safety systems). In this world, networks will become more open, dynamic, distributed, and expected to support many critical IT applications.

Network security is increasingly critical as the industry moves into the Internet of Things (IoT), 5G, and virtualization. Low-cost, high-volume IoT devices and the continuous trend towards open and virtualized environments increases the number of attack vectors into a network. Operators who provide a high-level of security and are able to address security gaps between networks will be the preferred choice by clients. The integrity and availability of these networks will also become a major national security challenge.

These challenges force the market to create a new security paradigm where all stakeholders – the government, operators, telecom equipment vendors, and IT players – need to reassess the current policy and security framework. The framework should evolve to cater to the changing information technology and telecommunications landscape. Navigating through these challenges will be essential for Kazakhstan in the light of wide-spread 5G introduction.

Ensuring security and privacy in 5G networks requires holistic security management. Understanding this, Ericsson provides security solutions that span networks, from access to core, with integrated management tools. The capabilities include fast network anomaly detection through its data analytics and adaptive security measures, which uses those same analytics to mold policy automation.

Ericsson has Two Types of Security Solutions:

RAN Security solution

The *Ericsson RAN Security* solution provides protection through authentication and encryption for the Ericsson Radio System and the broader network. The solution integrates and verifies all key components required to secure the radio and transport networks, with a particular focus on radio nodes deployed in untrusted, public areas. The solution also comprises a “*Security Gateway*” for *Public Key Infrastructure (PKI)* systems and certificate management.

Cloud Core Security Solution

Security threats and attacks to IP core networks are constantly evolving. This places more pressure on network operators to ensure that key network assets, services, and data in transit stay protected. The *Cloud Core Security* solution was created with this in mind and serves to protect network operators from new attacks. By introducing network security functions like intrusion detection and prevention and antivirus/malware filtering, organizations can better defend their systems.

Connection points are prime targets for attack. Location tracking, eavesdropping, identity theft, SMS interception, and the discovery of a network's topology are just some of the risks. To manage these threats, Ericsson's *Cloud Core* solution also includes perimeter protection and protection for interconnected mobile networks through internet gateways, firewalls, traffic domain separation (in the form of VLAN and VPN), access control, and node hardening.

Ericsson is a leader in 5G, pioneering commercial live networks with multiple operators in the US, South Korea, Europe, Australia, and the UAE. With a strong and flexible 5G portfolio, users can activate 5G in all main frequency bands and efficiently utilize their valuable spectrum assets. The core network is also fully ready to support 5G and Ericsson currently has 75 commercial 5G agreements with unique operators – 22 of which are live networks.

In addition, the *Ericsson Radio System* hardware has been 5G-ready since 2015 and can also be used for 5G NR (New Radio) with a remote software installation. In total, the company has shipped over 4 million 5G-ready radio units since then. This gives customers a unique advantage as it enables a smooth, secure network transition into 5G.

On 3GPP (the *3rd Generation Partnership Project*), Ericsson is dedicated to innovation and security as its lead contributor with approximately 50,000 papers on developing 2G, 3G, 4G, and 5G – 15,000 more than any other company in this community. The company has also achieved interoperability milestones with 3rd party partners such as Qualcomm to be the first in the industry across all main 5G frequency bands, which is necessary to secure 5G and realize its full potential.

This year (2019), Ericsson took the next step in enhancing its end-to-end (E2E) 5G platform through key portfolio launches across core, service orchestration, transport, and radio access. This also included Ericsson's dual mode *5G Cloud Core* portfolio, which created one common network for 5G and earlier network standards and installed standalone 5G software on its radios.

CYBERSECURITY FOR BUSINESS, PUBLIC SERVICES, AND INDIVIDUALS

by Andrey Gusakov

Head of Information Security Technology Consulting
Oracle CIS

Oracle's clients face the technological and legal challenges of a growing number of cybersecurity threats. Some customers would like to make data security "someone else's problem," and they are right, considering the lack of "Sherlock Holmes-level" professionals. In this context, that "someone else" is a tech-vendor able to design technology that is inherently more secure than what non-tech businesses could design for themselves. Research also shows that, while most companies cite "human error" as a leading cause of data breaches, they too are unaware of what technology can actually do for them. Oracle has reimagined "the Cloud," and its new high-performance Generation 2 offering has unmatched governance and security controls.

Oracle has built security into its products and protected its customers' data for decades. It provides the highest security for those who have trusted Oracle to manage their data and business-critical applications through its autonomous database. Oracle's Cloud is, therefore, secure by design through an integrated and layered approach with controls built within the application and database ecosystem to leverage the hardened Cloud infrastructure for threat identification and response – making its Cloud one of the most resilient against cyberthreats.

Machine learning-based adaptive intelligence is the future of cybersecurity

Today's diverse computing environments demand an intelligent security framework that can continuously monitor potential threats and challenge suspicious behavior. The goal is to eliminate false positives, minimize trivialities within millions of alerts, and allow the machines to handle the minutiae – like stepping up authentication measures automatically to prevent access by unauthorized users.

Oracle has a suite of Cloud-based services that brings greater visibility, intelligence, and automation to cybersecurity activities. All of Oracle's security services are built on the *Oracle Management Cloud (OMC)*, an integrated set of monitoring, management, and analytics services that leverage machine learning and big data technologies against a broad operational dataset. It enables rapid detection, investigation, and remediation of security threats and correlates the results with the privileges assigned in an *Identity and Access Management (IAM)* platform or *Active Directory*.

Oracle's *Orchestration Cloud Service* allows security administrators to automatically respond to issues, alerts, and events.

It also allows setup with custom rules to choose preferred scripting languages and software configurations. When Oracle's Cloud-based cybersecurity applications alert the database of vulnerabilities, the database can patch itself "on the fly." It can also detect anomalous *Structured Query Languages (SQL)* by parsing SQL statements to establish whitelist baselines by user, group, database, and application. It evaluates new SQL queries against this baseline to identify potential threats, raise threat scores, and take action to protect sensitive data. In addition, Oracle's *Autonomous Database Cloud Service* simplifies database administration and tuning tasks – such as automatically maintaining security configurations.

Shared responsibility

Top-tier Cloud providers are sufficient in securing their infrastructure, but customers are responsible for protecting their own data in the Cloud. Data breaches and attacks can occur even when companies have IAM systems. In addition, application programming interfaces (APIs) and user interfaces have IP addresses that can be accessed from outside of a trusted organization's boundaries. Because they are exposed, these assets are targets of attacks via the internet.



As part of Oracle's "defense in depth" capabilities, the *Oracle Database Security Assessment Tool (DBSAT)* helps identify areas where a company's database configuration, operation, or implementation introduces risks and recommends changes and controls to mitigate them. *DBSAT* is provided at no additional cost and enables customers to quickly find security configuration issues and determine how to remediate them.

Security configuration scanning and securing sensitive data are important aspects of regulatory compliance and are key to the *EU General Data Protection Regulation (EU GDPR)*, *Payment Card Industry Data Security Standard (PCI DSS)*, *Sarbanes-Oxley (SOX)*, *HIPAA/HITECH*, and numerous other data privacy laws. *DBSAT* recommendations help minimize risk, enhance the overall security posture of a company, and accelerate a company's path to compliance.

DBSAT also helps the user:

- *Discover Sensitive and Personal data in Oracle Databases*
- *Map Findings to the GDPR Articles/Recitals, the Oracle Database's STIG rules, and the Center for Internet Security's (CIS) benchmark recommendations*
- *Accelerate Data Protection Impact Assessments by assessing one's exposure to risk*
- *Recommend security controls such as encryption, segregation of duties, pseudonymization, and audits that assist in compliance*

DBSAT can be used whether a database is running on-premises, in customer-managed Database Cloud Services, or in IaaS (Infrastructure as a service) deployed databases, providing a simple way to assess the Oracle Database's Security posture in a consistent manner across hybrid deployments. Additionally, *DBSAT* supports database versions from Oracle 10.2 through Oracle 19c.



Customer Success Stories

Symantec & Oracle

As the largest pureplay security vendor in the world, Symantec delivers security solutions to approximately 85% of the world's Fortune 500. In partnership with Oracle, Symantec is delivering key components of its *Integrated Cyber Defense Platform*, optimized for the Oracle Cloud, so that customers can transition their databases.

Symantec & Oracle work closely together to build the Cloud architecture that ensure security of its infrastructure. The advanced security services and monitoring capabilities of this next-generation environment will ensure complete protection from the user's workstation to the Cloud application.

Lastly, Symantec is using Oracle's *Audit Vault* and *Database Firewall* to protect its customers' information and ensure PCI DSS compliance. This includes restricting inbound and outbound traffic based on the necessities of the cardholder's data environment; establishing an access control that is based on a "user's need to know" rule (it is set to "deny all" unless specifically allowed); and meeting all auditing requirements like SYS, Object, Login, Status.



The Ministry of Justice of Spain

Spain's Ministry of Justice oversees the consistent execution of the Nation's laws across the country's 23 provincial offices, all while coordinating funding and procurement for tribunals, magistrate courts, and prosecutor's offices. The Ministry also works to ensure compliance with data privacy laws in order to protect citizens' personal data (such as information about juvenile offenses and domestic violence cases) used by courts during legal and judicial procedures.

With the help of Oracle's Advanced Security, Spain's Ministry of Justice is now compliant to EU data privacy laws. This called for the encryption of over 400 million pieces of personal information — names, home addresses, lawsuits, court cases, and arrest records.

Together, the Ministry also established an access control and monitoring system that isolates user functions so that only authorized users can access or modify data. New logging procedures and time-stamping all accesses also mitigate the risk of data leaks and ensure user accountability.

Lastly, the Ministry used Oracle's *Data Masking and Subsetting Pack* to replicate and sanitize sensitive data in development and test environments. This enabled the Ministry to develop and test new applications without compromising sensitive information and reducing overall masking time from one week to only a few hours.

CYBERSECURITY FOR MOBILE OPERATORS IN KAZAKHSTAN

by **Kaspars Kukelis**
CEO, Kcell

The technological gap in mobile communication networks between Kazakhstan and most other developed countries is rapidly shrinking. This triumph, however, comes at a cost, as the risks to operators are now essentially the same as the risks faced by operators in developed countries, who are more experienced dealing with advanced Cyberthreats.

While the similarities between networks in Kazakhstan and those in other countries is growing, there are some key differences.

- *First*, with the rapid nature of development, most of the Kazakhstani population's value systems have yet to understand the value of digital information, and thus the average consumer is oblivious to or not capable of correctly assessing Cyberthreats.
- *Second*, complicated authentication and authorization systems cause clients to be bewildered and irritated, as the lack of ability to control one's own digital assets and entities leads to a delayed response to any Cyberattack. This delay, in turn, leads to increased damage from such strikes.
- *Third*, technological development in Kazakhstan is now accompanied by a change in business models from vertical to horizontal – where the services provided to the population changed from a monopoly to a multiplicity of operators, networks, and services.

Thus, one operator, along with access to other services, also provides access to threats that it cannot control on its own. The risks are managed on the basis of complex contractual relationships, such as converged network services, which only serves to further complicate an operator's response capabilities.



Kcell knows this frustration first-hand. In 2013, Kcell faced an attack on its web resources, where money was withdrawn from subscriber balances and then cashed out

through various payment systems. With the development of mobile financial services and their integration into the market, the number of these types of attacks will only increase. In response, it is necessary that the Government, with the participation of telecom operators, develop a system to increase public awareness of digital culture – both of threats and the means to protect oneself and one's organization from them.

This effort must also coincide with appropriate adjustments to the legislative framework to ensure effective and transparent protections for both the consumer and the telecom operator. Along with protecting their networks, perimeters and nodes, the purview of telecom operators should also include protecting services and preventing data manipulation.

Development of Cybersecurity in the 21st Century

The future brings the emergence of new threats associated with technological development. Trends in Cyberthreat capabilities show that implementation is becoming cheaper and “weapons” that bypass protections are becoming more anonymous and more standardized.



Part of this problem is the vulnerability of new systems. Introducing 5G technology and its related services require increasingly faster data transmission with low latency. Higher speeds, however, come with accelerated data leakage, and low latency will mean a delayed response to any attack. Even more worrisome is that mobile networks are still using insecure protocols such as SS7 and Diameter to route voice calls and data.

Another part of the problem is the *Internet of Things (IoT)*. The increase in communication subjects and the number of devices that constantly communicate through networks is projected to increase from 400 million to 1.5 billion due to IoT technologies.

This increase will undoubtedly amplify the number and types of vulnerabilities and threats related to authentication, authorization, and entity substitution.

Kcell is also wary of the future of cyberattacks. The company projects several trends. Containerized technologies (threats of “added” functionality) will undoubtedly create new attack vectors; strategies will broaden from distributed *Denial-of-Service (DDoS)* strikes to attacks on equipment and reputation; personal data will be a new priority target; companies will have to face an exponential increase in the number of small-scale attacks; and, lastly, new strategies will leverage insiders’ IDs or use technologies that allow criminals to convincingly “spoof” them.

With these concerns in mind, Kcell identified six recommendations for network operators to prepare for threats in the coming years.

- *First*, networks need to implement end-user level security measures on devices. This will better fortify the attack vectors into a network against end-user weak points.
- *Second*, telecom operators need to coordinate with each other and with government more effectively. This means creating information security coordination centers to manage common actions in combating large-scale threats.
- *Third*, operators need to invest in and implement autonomous security systems that are capable of quickly responding to suspicious account activity, leveraging advanced behavioral analytics.
- *Fourth*, operators should develop unique “defensive trap systems” by creating false targets for the attacker. With this tactic, the defender can better understand the attacker’s identity and intended target(s).
- *Fifth*, with the intense usage of Cloud technologies and services, companies need to better protect these virtual environments.
- *Last, but not least*, effective defense is a proactive measure. Operators need to constantly analyze their source code and identify vulnerabilities within it so that they can develop new defenses against attacks that actively seek to exploit those weaknesses.



INTRODUCING DIGITAL TRUST INSIGHTS

by **Vitaly Sokolov**
Partner, PricewaterhouseCoopers Russia

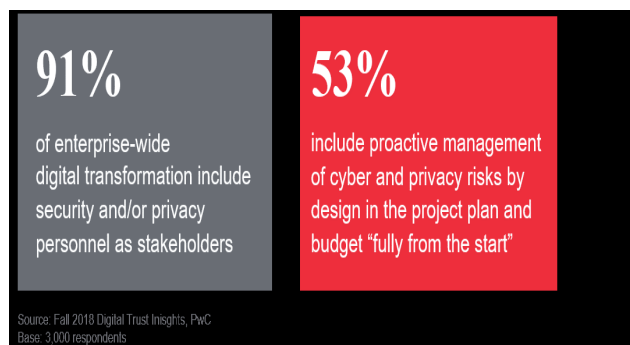
For 20 years, leaders have turned to PwC's *Global State of Information Security® Survey (GSISS)* as a trusted resource to navigate the cyber risk landscape. Over time, that landscape has evolved to be less about "information security" and more about managing digital risk. As cybersecurity, privacy, and data ethics become increasingly intertwined, organizations need an authority for research data and actionable advice. That is why PwC is rebooting GSISS to create Digital Trust Insights. This new platform will explore how to build confidence in the readiness of people, processes, and technologies to meet tomorrow's challenges.

Engage security experts at the start of digital transformations

Companies everywhere are pursuing digital transformation projects—putting emerging technology into action while aiming to solve problems, create unique experiences, and accelerate business performance. It's no secret that sprawling connectivity among personal devices, governments, businesses, and industrial equipment is fueling exponential growth in cyber and privacy risks.

Nine out of ten GSISS survey respondents at companies executing digital transformation projects say that security and privacy personnel are included as stakeholders and that their companies proactively manage cyber and privacy risks by design (within a project's plan and budget).

However, only 53% say that proactive risk management measures are integrated into the project "from the start." That percentage is higher in the financial services, health, and TMT¹ sectors and is lower in consumer markets (among respondents from medium and large companies). With this in mind, there is not one company here that does not have the opportunity for improvement – businesses worldwide can do better.



¹Technology, Media, and Telecommunications

Improve communications and engagement with the board of directors

Most respondents responsible for communicating with the board on cyber and privacy risks say that their company has provided the board with strategies for cybersecurity (80%) and privacy (83%). Many of these same businesses, however, may have doubts or concerns around their internal reporting on cybersecurity and privacy metrics. Only 27% of respondents say that they are very comfortable that the board receives adequate reporting on metrics for cyber and privacy risk management.



Actionable advice for business leaders

1. Know that the types of measures (implementation, effectiveness/efficiency, and impact) that are obtainable and useful for performance improvement depend on the maturity of the security program and how controls are implemented. Start with what can be measured today and create a plan to add more sophisticated metrics over time.
2. Also, metrics must address the needs of the stakeholder audience. The board might want metrics on the business impact of security activities—for example, the impact of security spending on overall risk posture, the cost of addressing a security event, or the impact of security efforts on public trust.
3. Communicate to the board how external factors—threats, third-party risk and regulations—affect overall risk posture and effectiveness of risk reduction.
4. Improve the CISO's² engagement with the board

Boost cyber resilience

Cyber resilience includes the agility of both defense and recovery capabilities. Resilient systems help companies sustain operations when possible amid cyberattacks and help rapidly recover in the event of a disruption. This is critical because crippled operations can lead directly to financial losses that often exceed, and mount more quickly than those from data exposure.

² Chief Information Security Officer (CISO)

The importance of maintaining data integrity will only grow as companies make more data-driven decisions with the aid of artificial intelligence. Only about half of medium and large businesses in key sectors say that they are building resilience to cyberattacks and other disruptive events, and fewer than half say that they are very comfortable that their company has adequately tested its resistance to attacks.

Actionable advice for business leaders:

1. Develop an understanding of the risk appetite around core business practices. Take into account the different views of stakeholders such as the chief financial officer, the chief operating officer, the chief information officer, and other executives focused on security, privacy, and risk.
2. Use leading approaches to cyber resilience. This includes developing and assessing plans designed to address risk-appetite concerns in an evolving threat landscape. It should also include monitoring the technology infrastructure to enable high availability, disaster recovery, and data integrity.

Be proactive in compliance

Respondents say that the greatest important challenges in digital compliance and ethics worldwide include the awareness of the latest regulatory developments (41%), compliance with current regulations (37%), and preparedness for future regulations (34%). Brazil's data protection law is a recent example of new legislation. Perhaps the most well-known example is the European Union's *General Data Protection Regulation (GDPR)*, which went into effect in May 2018. Fewer than half of all companies worth \$100 million or more that responded say that they are fully ready to comply with the GDPR.

Among US respondents, confidence about the readiness to comply with the *California Consumer Privacy Act*—which goes into effect in 2020—varies by sector: TMT companies are the most confident and health companies are the least confident. Three-quarters of respondents in China say they are entirely ready to comply with China's cybersecurity law, but far fewer respondents in other countries assert the same.

Actionable advice for business leaders:

1. Focus more on identifying new and emerging legislation, rules, and guidance on their implementation.
2. Use an integrated compliance approach instead of siloed efforts. In other words, businesses operating across different jurisdictions should comply with the highest standard. The boundaries of such an approach should be the sum of all the rules.

Accelerating controls for emerging technologies

Keep pace with innovation

Explosive growth in technology and data over the next decade will obliterate barriers between the cyber, physical, and virtual worlds, thus ratcheting up the complexity and scale of cyber and privacy risk management worldwide. Digital data and devices will be embedded more into critical infrastructure, consumer products, vehicles, daily life, and even in humans themselves, in a “world in which the physical, cyber and virtual merge.” Data collection will be more pervasive than ever as the internet of things (IoT) spreads like ivy—and hackers will be drawn to its vines like birds to its berries. Not surprisingly, most respondents (81%) say IoT is critical to at least some of their business. Only 39%, however, say they are very confident they are building enough “digital trust” controls—security, privacy, and data ethics—into their adoption of IoT.



Source: Fall 2018 Digital Trust Insights, PwC
Base: 3,000 respondents

In addition, only 30% list IoT security among the safeguards they plan to invest in this year. IoT devices interact with the physical world in novel ways. These devices often cannot be accessed, managed or monitored like other information technology, and they sometimes require additional cybersecurity and privacy controls.

Survey respondents have even less confidence in their digital trust controls for other emerging technologies such as artificial intelligence (AI). The allure of AI as an essential tool with a multitude of uses, such as predicting the rise of pandemics, driving autonomous vehicles, and augmenting cybersecurity measures, will pressure companies to implement it.

According to the survey, 70% of respondents say AI is critical to at least some of their business, but only 31% are very comfortable they are building enough digital trust controls into their adoption of it. Also, only 22% of all respondents say that they plan to invest in AI as a security safeguard over the next year. This percentage, however, is higher among medium and large companies as in TMT (46%) and financial services (40%). Such investments could one day transform the role of the CISO and provide ways to defeat otherwise unstoppable AI-powered cyberattacks and deception schemes.

Companies that commit to building and demonstrating new trust mechanisms in the crucible of today's business, risk management, and compliance challenges will likely define tomorrow's digital economy, crowding out less dedicated competitors.

Actionable advice for business leaders

1. Prioritize the development of digital trust controls and security budgets to support business investments and objectives around IoT, AI, and other emerging technologies.
2. Stay attuned to emerging IoT security research. For instance, Carnegie Mellon University (CMU) researchers at the Risk and Regulatory Services Innovation Center at CMU have been researching the development and design of new threat modeling, risk, and maturity assessment frameworks for IoT. Such frameworks could enable organizations to make more informed decisions about which actions and controls to implement for IoT security.
3. When creating software, do not simply integrate development and operations but embed security in the process (DevSecOps).
4. Recognize that AI will need both more robust governance and a new operating model.
5. Recognize that emerging research in quantum computing could have profound implications for cybersecurity. It is never too early to begin preparing.



Delivering Festive Joy Worldwide

sales@globalinklogistics.com | www.globalinklogistics.com



www.rixos.com
almaty@rixos.com

RIXOS
ALMATY

+7 727 300 33 00

SEPTEMBER BUSINESS ROUNDTABLE LUNCHEON WITH NATIONAL BANK GOVERNOR YERBOLAT DOSSAEV



Yerbolat Dossaev
Governor of the National Bank of Kazakhstan

Each year, AmCham invites the Governor of the National Bank of Kazakhstan to address AmCham members on banking policy and issues facing the banking community, with comments on the country's economic development. Newly appointed National Bank Governor, most recently Kazakhstan's Deputy Prime Minister, and a good friend to AmCham in his previous Cabinet positions, Yerbolat Dossaev spoke to members in the Rixos Hotel's Lotus Restaurant on 7 November.

Governor Dossaev began by outlining the banking topics he considered of most importance. He signaled the upcoming split of the National Bank of Kazakhstan and creation of the Agency for Regulation and Development of Financial Markets, Kazakhstan's macroeconomic situation, recent changes in anti-money laundering legislation, and the banking sector's Asset Quality Review.

Kazakhstan's Macroeconomic Situation

As the primary objective of the National Bank is price stability, since 2015 the Bank has adopted an inflation- targeting, free-floating exchange rate. As a result, the annual inflation rate has been decreased from earlier double-digit figures to just 5.5% as of October 2019. This is good progress towards achieving the inflation target of 4%-6% for 2020-2021 with a further reduction to 3%-5% in 2022.

As a part of its commitment to international trade policy, the National Bank uses the base rate as the key instrument to keep inflation within the target corridor. On 9 September 2019, the base rate was increased by 25 basis points to 9.25%. By the end of October, the base rate remained unchanged at 9.25% and inflation was projected to be within the target corridor mentioned previously. The National Bank expects inflation by year-end to be slightly closer to the upper-range of the inflation target (between 5.7% and 5.8%) with a projected slowdown in mid-2020 to 5.5%.

Kazakhstan's economic performance returned to strong, positive economic growth exceeding 4% annually over the past three years. Based on the first 9 months of 2019, real GDP growth stood at 4.3% due to strong positive growth across almost all sectors of the economy. Manufacturing, mining, construction, trade, and transportation were especially strong.

As of September 2019, the loan portfolio of banks amounted to 13.4 trillion tenge, an increase of 2.3% (303 billion tenge) from the beginning of 2019. The volume of loans to individuals from banks has also increased by 17.6% (6.2 trillion tenge). Loans to businesses, however, decreased by 8.1% (7.2 trillion tenge) in that same period. The decline in loans to businesses is a direct result of write-offs for non-performing loans in the first quarter of 2019. Starting from the 2nd quarter, credit has begun a strong recovery with the total loan portfolio increasing from April to September by 7.4% (922 billion tenge). The increase in credit to businesses was 1.7% (122 billion tenge), while to individuals the increase was 14.7% (800 billion tenge).

As of 1 October, concerning Kazakhstan's sovereign debt, the external government debt amounted to 15.2 billion USD or just 8% of Kazakhstan's GDP. With such low sovereign debt, Kazakhstan is in a strong net asset position, given that Kazakhstan's international reserves amounted to 88.2 billion USD. This breaks down to 28.8 billion USD in the National Bank's foreign exchange reserves and 59.4 billion USD in the National Fund.

In the first half of 2019, Kazakhstan experienced a relatively small current account deficit – 1.9 billion USD or 2.4% of GDP. This is in contrast to the nearly balanced current account by the end of last year with the deficit only amounting to 289 million USD – 0.2% of GDP. This increase in the current account deficit is related to higher import growth driven by significant fiscal stimulus. Imports were also supported by the fast pace of Kazakhstan's investment projects, mainly consisting of equipment and machinery for large oil and infrastructure projects. The continued expansion of production from Kazakhstan's largest oil fields will allow the country to increase its export potential in 2022 and onwards.

Although this high level of importation exerts pressure on the current account, it will ultimately help stimulate economic growth and development, which will rebalance Kazakhstan's accounts. Infrastructure projects will also help local businesses by improving logistics capabilities and decrease transportation costs across the entire economy. As for Kazakhstan's capital accounts, the National Bank notes a steady inflow of foreign direct investment (FDI). In the first half of 2019, gross FDI into Kazakhstan amounted to 12.1 billion USD, a 3.1% decrease compared to the same period from the previous year (12.5 billion in the first half of 2018).

The Split between the National Bank and the Agency for Regulation and Development of Financial Markets

National Bank Mandate 2019

The National Bank has a wide mandate for financial sector supervision and implements best practices to foster better compliance with supervisory decisions. In July 2019, the supervisory mandate of the National Bank expanded to include not only the banking sector, insurance companies, and non-banking financial institutions, but also financial organizations previously outside the scope of regulation, such as online lenders, credit partnerships, and pawnshops. This aimed to resolve the uncontrolled growth of consumer lending in unregulated sectors to protect the rights and interests of the borrowers from unregulated lenders. As a control and supervisory measure, the law introduced special requirements depending on the risks inherent in a particular type of activity.

National Bank also determined that microfinance entities required more oversight and regulation to eliminate over-lending. In particular, the law placed requirements prohibiting the collection of fees and forcing lenders to comply with marginal interest rates. These measures improved the transparency of the lending market, eliminated existing imbalances in the regulation of various segments, and most importantly, protected borrowers' rights.

Throughout 2019, the banking sector was the focus of increased regulation, supervision, and oversight. It is clear now that effective management of this sector necessitates decision-making free of conflicts of interests. To achieve this goal in 2020, the government is establishing a new, independent financial supervisory agency – the *Agency for Regulation and Development of Financial Markets*.

Agency for Regulation and Development of Financial Markets Mandate 2020

As of 1 January 2020, the financial supervisory mandate (a competency of the National Bank) will become the responsibility of the *Agency for Regulation and Development of Financial Markets*. The Bank is currently working to prepare for this split. The separation of functions between the National Bank and the new regulatory agency will help eliminate conflicts of interest, promote risk avoidance, and eliminate unfair practices in the financial sector. The Agency will be responsible for all regulatory responsibilities formerly under the purview of the National Bank, including the aforementioned additions to the mandate in 2019 – the unregulated actors in the banking sector.

The Agency will also be tasked to develop more types of financial services, establish a securities market, and facilitate greater financial inclusion. Even with the split, the National Bank retains its mandate on monetary policy, financial stability and macroprudential policy, payment systems, currency money circulation, and other functions associated with a traditional central bank. Meanwhile, the Financial Stability Council will act as a coordinating body for financial stability, macroprudential policy, crisis prevention and resolution.

The Asset Quality Review (AQR)

Alongside preparations to establish the new independent regulatory agency, the National Bank is implementing a new risk-based approach to supervision. The key element is supervisory judgment, a response to the risks in the banking sector applied in the following areas:

1. *Approval of management and shareholders;*
2. *Identification of related parties;*
3. *Assessment of the adequacy of provisions (reserves);*
4. *Assessment of risk management systems and internal control.*

As the starting point for this risk-based approach, the National Bank is conducting the AQR. This review will be in line with the best practices of the European Central Bank (ECB) and will provide an independent perspective on the current banking situation.

The AQR pursues three main objectives:

1. *Ensure transparency throughout the entire banking system by improving the quality of available information about the financial condition of key banks;*
2. *Strengthen financial stability by identifying and implementing corrective measures to improve the financial condition of banks (if necessary);*
3. *Increase investor and depositor confidence in the reliability of banks operating in Kazakhstan.*

In order to ensure the transparency and objectivity of the assessment itself, the AQR is executed in conjunction with international consultants and independent auditing companies. The assessment of Kazakhstan's banking sector will be conducted according to ECB methodology, which guarantees uniform international quality standards and encourages the international community's confidence in the results. At the same time, the ECB's methodology was adjusted to accommodate the specifics of Kazakhstan's financial institutions' legislative and business processes.

The AQR began in August 2019 and includes 14 banks accounting for 87% of the banking sector's assets. As of October, the National Bank completed 3 out of 10 AQR stages:

- *First, an analysis of the results of bank policies and processes was completed;*
- *Second, recommendations were made based on the analysis;*
- *Third, a review and collateral valuation based on the loans' sample credit file was completed.*

The AQR should be completed in December 2019, and the results will be made available to all banks participating in this assessment. Based on the results, an action plan will be drawn up, if necessary, for corrective measures, and recommendations will be made to banks that need to improve their business processes. The National Bank has not received complaints concerning the AQR, but, as always, it is ready to listen to the business community and to address their concerns on a case by case basis.

Anti-money Laundering and Countering the Financing of Terrorism (AML / CFT)

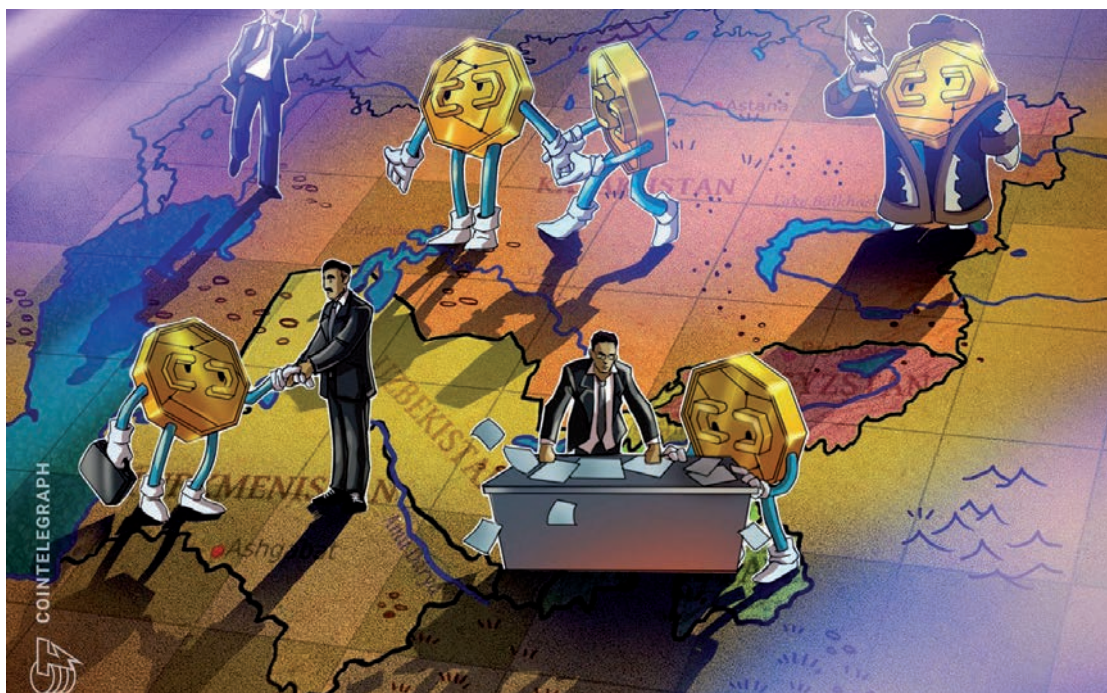
The National Bank understands the damage caused by money laundering and the financing of terrorism. These threats have ceased to be shortcomings of one particular

financial institution and have become challenges to the stability of the entire financial system. The National Bank integrates AML/CFT supervision into its risk-based supervision system to intensify protection for shareholders and owners of financial institutions.

In this new era marked by a proliferation of digital services and the development of financial technologies, the National Bank supports the FATF and OECD initiatives to control AML/ CFT risks on financial markets. The Bank is also studying international best practices to monitor FinTech companies, as well as electronic money and digital cryptocurrencies to eliminate gray areas of financial supervision.

In addition, the New Law "On Currency Regulation and Currency Control" came into force this past July. The new law expands monitoring and oversight of foreign exchange operations. There are also more plans to further strengthen AML/CFT supervision regarding non-cash conversion transactions to comply with international best practices. This means that large conversion operations must be subject to due diligence (i.e. sources of money, the beneficiary/ beneficiaries, and the customer's reputation).

The above requirements are prudent and preventive in nature and do not entail any restrictions for a bank's clients. Above all else, the National Bank of Kazakhstan remains committed to the principles of a liberal currency regime that does not restrict foreign currency transactions.



AMCHAM SEPTEMBER BUSINESS ROUNDTABLE WITH AMBASSADOR STEPHEN DE BOER, CANADA'S WTO REPRESENTATIVE



Ambassador Stephen de Boer, Canada's WTO Representative

AmCham was pleased to welcome Ambassador Stephen de Boer, Canada's Permanent Representative to the WTO, as our guest speaker for the September Business Round Table on September 20 at the Lotus Restaurant in the Rixos Almaty Hotel. His topic was reform and modernization of the World Trade Organization.

Stephen de Boer joined Global Affairs Canada in 2005, where he has held various positions, including in the Investment Trade Policy and North America Trade Policy Divisions. In 2010, he joined Environment Canada as Deputy Chief Negotiator for climate change and Director General responsible for Canada's international climate change partnerships. He returned to Global Affairs Canada in 2013 as Director General of the Trade Controls Bureau, receiving his first ambassadorial appointment in 2015 as Ambassador to Poland, then Ambassador to Belarus the following year. In 2017, Ambassador de Boer was appointed to his current position as Permanent Representative to the WTO in Geneva.

Ambassador de Boer's speech focused on the current state of affairs within the WTO and between its member countries in the prelude to the highly anticipated WTO MC12 meeting in June, hosted by Kazakhstan. Reviewing WTO major issues, he outlined Canada's position post-Doha to reform WTO and suggested how Kazakhstan and the private sector can contribute.

The WTO is almost 25 years old and much has changed in the world since its founding. When the WTO came into existence, the internet was in its infancy; China's economy was only beginning its meteoric growth; and the world was much less multipolar than it is today with the U.S. as the world's only true superpower. Now the internet is omnipresent; China, India, and Brazil are all increasingly assertive and important economic actors; and the United States has retreated from its traditional role as chief defender of the multilateral trading system.

Trade liberalization and globalization have become flash points in the backlash over the increasing inequalities and societal challenges facing the world. This backlash manifested itself in outcomes such as Brexit; the "gilet jaune" protests in France; and the results of the 2016 U.S. presidential election - events reflective of a discontent that has been building for years. Why has trade been a flash point or a scapegoat for many of today's challenges? The multilateral trading system has displayed notable failures over the last 20 years or so – most notably, the WTO's Doha round.

Launched in late 2001 to great fanfare and optimism, the mandate for the Doha negotiations was ambitious, including issues concerning agriculture, services, and non-agricultural market access, trade and environment, among others. One of the fundamental objectives of the Doha Round was to improve the trading prospects of less-developed countries and to help them better integrate into global trade, placing the multilateral trading system on a solid footing for the 21st century. In addition, China had just joined the WTO, the world was keen to demonstrate cooperation and unity following the 9/11 attacks, and the Doha round intended to successfully address most of the persistent economic challenges such as agricultural subsidies. 18 years later, and despite coming close to reaching an agreement, it is clear by any objective measure that Doha has failed.

It failed for many reasons – one was that all issues were addressed as a single undertaking, thus nothing is agreed until everything is agreed. This approach is too difficult and ambitious to realistically expect success. Canada believes that new models or approaches to negotiations at the WTO are needed – not a single undertaking approach. Some WTO members, especially smaller and/or developing members, are keen to preserve the single undertaking model, seeing it as their only guarantee that the issues important to them will be addressed.

The reality, however, is that only a very small number of issues are being advanced multilaterally. More importantly, it is impossible to formally pursue new issues or approaches to negotiations as this would require the consensus of all members. Meanwhile, as WTO members continue to bicker about how to move negotiations forward, time marches on.

The world of commerce today is ever more complicated; integrated, and sensitive to stakeholder expectations. Countries have responded to these realities by negotiating modern bilateral or regional trade agreements – the CETA, the CPTPP and CUSMA are only three examples of such recent Canadian agreements. These modern agreements, however, are underpinned by the WTO. In other words, the majority of global trade still rests on the shoulders of WTO rules. Although the WTO is a vital institution

in global governance – one that must be preserved – its rules, functions, and procedures must match the needs and expectations of 21st century stakeholders. These stakeholders include business, government, and civil society, all of whom have vested interests in the WTO and its work. The challenge is determining what rules and procedures need updating and how best to achieve this.

The challenge is how to create the common cause necessary between a divided and diverse membership to pursue reform and to ensure WTO relevance and responsiveness in the 21st century. Reaching an agreement on what specifically needs to change remains a challenge.



These circumstances require concerted action and engagement from all WTO members. For a medium-sized country like Canada, the WTO constitutes a critical part of its international trade policy engagement. It provides a base from which to discuss concerns on trade policy issues with other members; to advance trade priorities; and to defend Canada's interests through dispute settlement.

More broadly, the WTO underpins Canada's bilateral and regional trade agreements, and is also an integral piece of international multilateral governance. Canada's support for the WTO is unwavering, and the country is taking concrete steps to help preserve the continuing relevance of the WTO.

ACTION

There are numerous opportunities for WTO reform, which is a broad topic and not limited to the crisis over the WTO's Appellate Body. The impasse over naming replacements to the WTO's Appellate Body has garnered significant media attention. This would have significant and serious consequences, which further compromises confidence in the WTO. However, the rest of the dispute settlement system will continue to function as members will still be able to file cases; panels will still be formed; and decisions will still be rendered.

The private sector is one of the key stakeholders in the effort to reform WTO. Private sector voices need to be heard on the importance of the WTO and the need for all governments to engage in an open, pragmatic and realistic discussion about preserving and modernizing the institution. Without the vocal support of the private sector, effecting meaningful change will be difficult.

Overall, the Spring / Summer 2019 meetings resulted in constructive discussions. To reach an ambitious outcome with a broad participation, the involvement and the support of all stakeholders, including the private sector, will be important.



AMCHAM THANKSGIVING CELEBRATION 2019

The AmCham Thanksgiving Celebration is the second of AmCham's two large family holiday celebrations each year – the first being U.S. Independence Day in July. The American Thanksgiving at the end of November is a holiday normally celebrated at home with turkey, seasonal vegetables, and pumpkin pie. Some family gatherings vary this classic Thanksgiving menu, but AmCham maintains all the Thanksgiving touches that remind members of this beloved holiday in their childhood.

The 2019 Thanksgiving was celebrated on 29 November at the InterContinental Almaty Hotel, where the Ballroom overflowed with 300 guests at corporate and group tables with friends, colleagues, and family. Jason Craig, Director of the Almaty International School, delivered the traditional Thanksgiving Welcome before Dinner.

The InterContinental Chef offered the classic Thanksgiving menu with some additional dishes for those guests whose tastes encompassed other specialties such as salmon and a broad array of desserts.

Children had their own menu outside the Ballroom with clowns and children's performers who entertained the younger guests while their parents enjoyed a quiet dinner (but it's never too quiet at a family Thanksgiving!) with Almaty's favorite jazz singer and AmCham's favorite jazz group providing lively backgrounds music.

The Thanksgiving Lottery after dinner offered a broad range of lottery prizes – brunches and dinners, spa vouchers, Herbalife gifts, and best of all, three airline travel prizes for couples to distant locations from Air Astana, Lufthansa, and Delta Airlines (soon to launch operations from Kazakhstan).





Contributing Sponsors:



AMCHAM ALMATY SEPTEMBER SUNDOWNER AT THE ST. PIERRE RESTAURANT

On 20 September, AmCham launched the Autumn Business Season in the run-up to the traditional Almaty KIOGE Oil and Gas Exhibition at one of Almaty's favorite restaurants, the St. Pierre Restaurant, well-known for its outstanding fish menu and well-stocked *vinothèque* adjoining the restaurant. A guitarist provided background music.

Sponsored by Chevron, whose Chief Executive Officer, John Baltz (an AmCham Board Member), welcomed the Sundowner guests, the evening was attended by 150 guests, including U.S. Consul General Eric Meyer. The first Sundowner of the Autumn is always an exciting event as members returning from their summer vacations gather to see friends and colleagues.

Chevron is one of the world's leading integrated energy companies. Chevron and Tengizchevroil gave birth to Kazakhstan's Tengiz oilfield and the oil industry that grew out of it, today serving as Kazakhstan's economic base. Chevron also holds a stake in the Karachaganak oilfield and is the largest private shareholder in the Caspian Pipeline Consortium.

Globally, Chevron plays a major role in Kazakhstan's history, but continues to pursue new projects for the country's future. When implemented, the *TCO Future Growth Project-Wellhead Pressure Management Project* will increase Tengiz crude oil production capacity by approximately 12 million tonnes per year or 160,000 barrels per day, an important milestone for Chevron and Kazakhstan.



AMCHAM ATYRAU OCTOBER SUNDOWNER AT THE RENAISSANCE ATYRAU HOTEL

AmCham held its annual *Autumn Atyrau Sundowner* on 4 October at the *Renaissance Atyrau Hotel* sponsored by ILF Kazakhstan. The Renaissance provided impeccable service and an outstanding buffet dinner in its Ballroom for the AmCham guests. Both Renaissance Hotels in the Caspian Region – in Atyrau and Aktau – are points of reference for AmCham members in the oil industry.

ILF Kazakhstan is a long-time AmCham member celebrating the opening of its Atyrau office to mark its newly-awarded contract for services to Tengizchevroil and its expanded operations in the Caspian region. The turnout for the Sundowner was large to mark this important occasion.

Founded in Austria in 1967, *ILF Consulting Engineers* is a leading European engineering and project management consulting company with 40 global offices. It has operated in Kazakhstan since 1994, supporting clients in the oil and gas industry.

Talgat Temirzhanov, Managing Director of ILF Kazakhstan delivered a warm Welcome to the Sundowner guests, outlining ILF's history, both in Kazakhstan and abroad, services and innovations, with a look forward to supporting Tengizchevroil in its major production expansion under the *TCO Future Growth Project*.



AMCHAM OCTOBER NUR-SULTAN SUNDOWNER AT THE MARRIOTT ASTANA HOTEL

Following the *AmCham Cybersecurity Conference* on 23 October, AmCham held a Sundowner in the *Marriott Hotel's Vista Lounge Bar / Restaurant* on the Hotel's top floor. Famed for its panoramic view over the city, especially at night when the city's towering buildings are flood-lit, the Sundowner was attended by Conference speakers and participants, diplomats, and AmCham members.

The diplomatic attendance was especially strong as AmCham had held its monthly Prime Minister's Council session the previous day. Together, the Council and the Conference had created a critical mass of attention on the need to increase Cybersecurity in Kazakhstan.

With the creation of the new Ministry of Digitalization and Innovation, it is hoped that new, enhanced legislation will soon be enacted to guide the Government of Kazakhstan in strengthening its own cybersystems to support and protect the Government's current high-priority *Digital Kazakhstan Initiative*.

The Sundowner was a fitting end to an intense day of discussion by Ambassadors, Cabinet Ministers, CEOs, and Cybersecurity experts. Relaxing with a glass of wine, music, and a glorious evening view over Kazakhstan's capital city brought the AmCham Nur-Sultan community together to discuss future advocacy initiatives.



ALMATY HALLOWEEN SUNDOWNER IN THE CIRCUS NIGHTCLUB AT THE ROYAL TULIP HOTEL

The *AmCham Halloween Sundowner* was held on *Friday evening, 31 October*, in the *Circus Nightclub* at the top of the *Royal Tulip Almaty Hotel*, which also sponsored the Sundowner. As always a fitting location, the Nightclub's dark, spooky interior, baroque golden chandeliers, circular niche seating around big group tables, winding stairs leading up to a mysterious mezzanine, huge screen for Halloween movies (this year Mel Brooks' *Young Frankenstein* and the *Time Warp Dance* from *Rocky Horror Picture Show*), the Club offered a spacious dance-floor for members ending the evening in style.

Face-painted Hotel waiters and waitresses served a Halloween menu and poured copious amounts of champagne while DJs spun Halloween music and sound effects in the background to set the stage for the occasion.

Although the Halloween Sundowner is a no-costume event, maintaining the semi-nature of the evening as a business and social networking event, members entered fully into the spirit of the night, enjoying a holiday that has become an occasion for revelry worldwide.



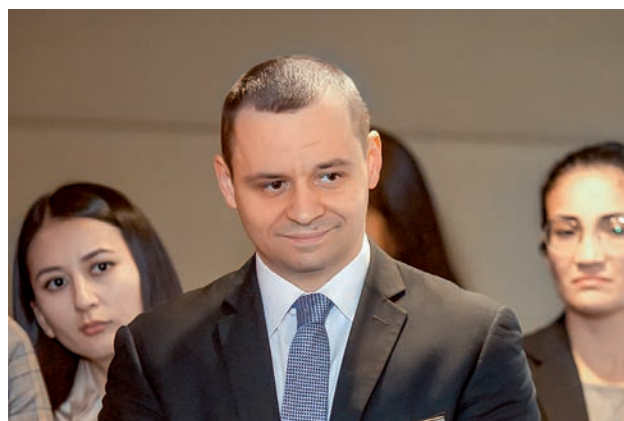
AKTAU NOVEMBER SUNDOWNER AT THE RENAISSANCE AKTAU HOTEL

The *AmCham Aktau Sundowner* on Friday evening, 8 November, was held in the cozy Lounge Bar at the Renaissance Aktau Hotel. Together with the Renaissance Atyrau Hotel, the two Renaissance Hotels offer five-star accommodations and services in the Caspian region that have made them the favored base for AmCham members. The Renaissance Aktau prepared a sumptuous seasonal buffet dinner with free-flowing wine and beer for the oil industry and its partners in the Caspian region.

Sponsored by *nVent Thermal*, the Sundowner had an impressive turnout of over 100 AmCham members and guests, a record for Aktau. After Dorin Baru, the OMV

Petrom CEO and official AmCham Representative in Aktau, delivered a warm welcome to Sundowner guests, *Peter Butterworth*, the *nVent Thermal Business Development Director*, spoke about nVent Thermal's operations and services focused on electrical heat management systems.

An outgrowth of Raychem, the nVent heat tracing systems are widely used in the oil and gas and mining industries. Petrochemical plants, refineries, and power generation plants also rely on nVent Raychem systems. The company is a major supplier and partner for the oil industry in the Caspian region.



ALMATY WINTER HOLIDAYS SUNDOWNER HELD AT THE INTERCONTINENTAL HOTEL J BAR

AmCham held its final Sundowner for 2019, the Winter Holidays Sundowner, on Friday evening, December 13, in the cozy and welcoming InterContinental Hotel J Bar to bid farewell to its members heading homewards for the Holidays. Ensnared on sofas and plush armchairs around the J Bar fireplace and listening to cool jazz, as befitting the location, AmCham members sipped wine, nibbled on hors-d'oeuvres, chatted about their Holiday plans, and looked forward to 2020.

The InterContinental Hotel is renowned for its Holiday decorations – the towering, sparkling fir tree in the Atrium, the Holiday Market with its array of gifts, the extravagant Holiday cakes and confections for Holiday tables, and

the pianist creating a Holiday musical atmosphere on the Lobby's baby grand piano – everything for a unique and joyful Holiday atmosphere.

AVON, a long-time AmCham member, very generously brought packaged gifts for the evening's guests. With a new General Manager for 2020, Mateo Lecocq, AVON will begin the New Year on new footing and undoubtedly with new plans in mind. We look forward to our continuing partnership with AVON and the other Direct Sales Companies.

And so AmCham brought its members together for a final toast to 2019 and with best wishes for 2020, when we will see our members again for another successful year.





Philip Morris International Appoints New Managing Director for Kazakhstan and Central Asia



Juan Carlos Escobar, newly appointed Philip Morris International Managing Director (PMI) for Kazakhstan and Central Asia, is originally from Spain. He joined the PMI Operating Center in Switzerland in 2004, following a career in Strategic Consulting in the UK and Australia.

Mr. Escobar has held numerous leadership positions in strategic planning, business development, fiscal affairs, international trade and commercial and general management, spanning EEMA (Eastern Europe, Middle East and Africa), Latin America and Canada. He holds an MBA from INSEAD Business School in France, as well as a Business Administration and Economics degree from ICADE University in Madrid.

About Philip Morris Kazakhstan:

Philip Morris Kazakhstan (PMK) is an affiliate of Philip Morris International (PMI), with a modern production facility in the Almaty region. Today, PMK is among Kazakhstan's TOP-10 taxpayers, to date paying over 2.7 billion USD.



Cameco Kazakhstan Appoints New General Director



Dmitry Barsukov was recently appointed General Director of Cameco Kazakhstan, a subsidiary of Cameco Corporation - one of the world's largest providers of the uranium needed to generate clean, reliable baseload electricity around the globe.

Mr. Barsukov has over 25 years of experience in mining, oil & gas, and the nuclear industries, both in operations and on major capital projects in North America and Central Asia. Prior to heading Cameco Kazakhstan, he served as Vice-President, Supply Chain Management at Cameco Corporation's head office in Saskatoon, Canada. Since 2016 he has been a member of the Supervisory Board of JV Inkai – a uranium-producing joint venture between Cameco Corporation and Kazatomprom with operations in the Turkestan region of Kazakhstan.

Dmitry Barsukov graduated in Economics from Kyrgyz National University and received an MBA degree from Richard Ivey School of Business at the University of Western Ontario. He holds the ICD.D designation from the Institute of Corporate Directors of Canada.



MEMBER NEWS

NEW MEMBERS

Takeda - Biopharmaceutical Innovation in Kazakhstan

2019 is important for the healthcare sector in Kazakhstan, with several major changes in the country's healthcare system and new important regulations. Kazakhstan's health care authorities are working to reform models of healthcare insurance, pricing, and improvements in health technology assessment implementation.

Another major change in the pharmaceutical sector is the merger of pharmaceutical leaders: Takeda completed its acquisition of Shire, a major biopharmaceutical company, for \$US 62 billion, thereby becoming a global pharmaceutical leader. Takeda now is the only pharmaceutical company listed on both the Tokyo and New York stock exchanges and is represented in 80 countries across the globe.

Takeda focuses its R&D efforts on four therapeutic areas: *Oncology*, *Gastroenterology (GI)*, *Rare Diseases*, and *Neuroscience*. The company also makes targeted R&D investments in *Plasma-Derived Therapies* and *Vaccines*.

In Kazakhstan, Takeda focuses on bringing innovations to the country's healthcare system. The company's main achievements are innovative treatment for *Crohn's disease*, *ulcerative colitis*, *Hodgkin Lymphoma*, *Hunter Syndrome*, *Hemophilia*, and *Multiple Myeloma*. Takeda works closely with local healthcare professionals in order to ensure disease and treatment awareness in these socially important therapeutic areas.

Recently Takeda opened new facilities designed for patients and health professionals at the *Kazakhstan Cardiology and Internal Diseases Research Institute*. Several years of joint work with the Government have resulted in draft guidelines for oncology treatment, and the world's first per-oral treatment for *Multiple Myeloma*.

Takeda continues to support medical education and has supported major conferences and congresses such as the *Kazakhstan Immunology Congress* and the *Uzbekistan Hemophilia Congress*. Takeda has also provided a successful webinar on Hunter Syndrome and launched a dual educational program with the *Pharmaceutical School at Kazakh National Medical University*.



Better Health, Brighter Future

There is more that we can do to help improve people's lives. Driven by passion to realize this goal, Takeda has been providing society with innovative medicines since our foundation in 1781.

Today, we tackle diverse healthcare issues around the world, from prevention to life-long support and our ambition remains the same: to find new solutions that make a positive difference, and deliver better medicines that help as many people as we can, as soon as we can.

With our breadth of expertise and our collective wisdom and experience, Takeda will always be committed to improving the future of healthcare.

Talan Towers Opens First Tesla Supercharger Stations in the CIS



On November 13, six Tesla Supercharger stations were opened in Nur-Sultan at the multifunctional Talan Towers complex, conforming to the green building standards of the GOLD category for the international Leadership in Energy and Environmental Design system (LEED®).

Talan Towers is the first building in the CIS to offer the most advanced infrastructure for Tesla electric vehicle owners. The Tesla Supercharger station will be available to all visitors to Talan Towers Offices and The Ritz-Carlton Hotel, Astana, as well as to all Nur-Sultan residents and guests.

The launch of this Tesla Supercharger station is the next step in the Talan Towers and Verny Capital Group green building strategy.

Verny Capital CEO Erlan Ospanov and Regional Tesla Charging Manager Dennis Schoenmakers opened the launch ceremony attended by the media, business partners, and guests. The speakers emphasized the Tesla Supercharger energy efficiency and environmental friendliness, and spoke about their future plans to promote a green infrastructure for electric transport in Kazakhstan.

"The idea of building our complex is to respect the environment and to create comfortable conditions for work and leisure. We are sure that not only owners of electric cars will benefit from this, but also all citizens, because the charging stations create infrastructure for an environmentally friendly capital in the future. Electric cars will make the air cleaner by reducing harmful emissions. We are very pleased that Talan Towers is at the forefront of Kazakhstan's development of green technologies", said Erlan Ospanov.

Initiatives like this are very important because the infrastructure for electric vehicles in Kazakhstan is just beginning to develop. According to KazAutoProm, from 2014 to 2017 there were only 119 electric cars in the country. The widespread availability of electric vehicles is hindered by lack of the necessary infrastructure for charging and maintaining these vehicles



WELCOME ADDITIONS TO THE CHAMBER



Delta Airlines

Discovery

International Organization for Migration (IOM)

CORPORATE A

CORPORATE A

NON-PROFIT

Leonid Tarasov
General Representative for Russia
and the CIS

Hester Wheeley
Senior Vice President – EMEA

Zeynal Hajiyev
Regional Chief of Mission

Millenium Park Business Center
26 Amanzholov Street, Block A,
Office 201
Nur-Sultan 010000, Kazakhstan

Discovery House
566 Chiswick High Road
London W4 5YB, United Kingdom

14 Azerbaijan Mambetov Street
Nur-Sultan 010000 Kazakhstan

Telephone: +7 7172 91 28 25
E-mail: maral.zhunussova@delta.com
Website: www.delta.com

Telephone: +44 20 8811 3000 (UK)
Email: Ekaterina_Mihajlovic@discovery.com
Website: www.corporate.discovery.com

Telephone: +7 727 258 26 43, +7 727 258 26 46
Email: iomalmaty@iom.int
Website: www.iom.int

As the world's most profitable airline according to the Fortune 500, Delta Airlines is a premier international travel service. Delta's mission is to become a force for positive local and global change, dedicated to bettering standards of living and the environment where the Delta team and its customers live and work.

Discovery (formerly **Discovery Communications**) is an American mass media company founded in 1985 based in New York City. Discovery has an annual revenue of \$11.1 billion and employs approximately 9,000 employees worldwide. It is listed on the S&P 500 and is traded on NASDAQ.

The International Organization for Migration (IOM) is the principal intergovernmental organization working in the field of migration. Its mission is to assist in meeting the growing operational challenges of migration management; to advance the understanding of migration issues; to encourage social and economic development through migration; and to uphold the human dignity and well-being of migrants.

Founded in 1929, Delta now has a fleet of over 800 aircraft – the second largest – globally serving nearly 200 million people every year in 325 destinations across 52 countries. Delta Airline's main hub is Hartsfield–Jackson Atlanta International Airport – one of the world's busiest, and, across its entire global network, Delta operates 5,400 flights daily, has annual global revenue of \$44 billion and 86,000 employees worldwide.

With over 8,000 hours of programming each year and a viewership of 2.8 billion subscribers worldwide across 220 countries and in 50 languages, Discovery's international popularity is well-known through its channels, which include the *Discovery Channel*, *Animal Planet*, *Science Channel*, *TLC*, *Food Network*, *HGTV*, and the *Travel Channel*.

Founded in 1951 to help resettle people displaced by World War II as the Intergovernmental Committee for European Migration, today IOM is an official UN-affiliated organization that deals with issues surrounding internally displaced persons, refugees, and migrant workers with 173 member states and 8 observer states.

As a founding member of the SkyTeam alliance, Delta further augments its service through its international partnerships. Delta currently operates flights from Moscow and plans to open new routes from Kazakhstan within the next year. Delta is represented in Kazakhstan by AviaReps in Nur-Sultan.

Discovery has three major regional operations outside North America: Asia Pacific; Europe, the Middle East, and Africa (EMEA); and Latin America. It also has regional headquarters in Miami, London, Milan, Singapore, Amsterdam, and Warsaw.

The IOM global headquarters in Geneva employs 11,500 staff worldwide. In Kazakhstan, IOM's regional Nur-Sultan office coordinates its efforts within the country and throughout Central Asia.

AMCHAM ADVOCACY UPDATE

SEPTEMBER - DECEMBER 2019

The Council to Improve the Investment Climate resumed its monthly meetings after a six-month hiatus marked by Kazakhstan's political transition that began with the dismissal of the Cabinet of Ministers and the Prime Minister at the end of February. President Nazarbayev's announcement in March that he would step down as President of Kazakhstan, was followed by the appointment, then election of his Presidential Successor, *Kasym-Jomart Tokayev*. Within a few days, the formation of a new Cabinet with a new *Prime Minister, Askar Mamin*, was announced. New Government appointments continued throughout the spring and summer at a frequently dizzying pace.

The rapid changes that marked this transitional period were felt to be a distraction from AmCham's ability to pursue its advocacy agenda, but by September the transitional process had stabilized. In April AmCham met with Prime Minister Mamin soon after his appointment to reconfirm the Government's intention to continue the *Prime Minister's Council to Improve the Investment Climate*, the Council created for AmCham and its members ten years ago. The Prime Minister confirmed that he regarded the Council as a valuable platform for dialogue with the foreign investment community, and that he wished to continue its monthly schedule of meetings in the autumn.

September Council Session: Kazakhstan's WTO Membership – A Review of Selected Issues

In light of the *World Trade Organization Ministerial Council (MC12)* to be hosted by Kazakhstan in Nur-Sultan in June 2020 – the WTO Ministerials are the WTO's highest decision making-body – it was decided to devote the first AmCham Council session in the autumn to reviewing Kazakhstan's commitments under its WTO Accession five years ago. Many of the commitments made at that time have not been fully realized. Thus, MC12 offers an excellent opportunity to revisit commitments that are important to Kazakhstan's investment community.

The June 2020 MC12 is very important for Kazakhstan as the country's ability to successfully host this prestigious event is a point of pride and is expected to catapult Kazakhstan onto the world stage. The new Trade and Integration Ministry will oversee logistics planning.

For the WTO session, AmCham and the Canadian Embassy invited *Canadian Permanent Representative to the WTO, Ambassador Stephen de Boer*, to travel from Geneva as a Guest Speaker. The U.S. Embassy invited *Zeba Reyazuddin, Deputy Assistant U.S. Trade Representative for Central Asia*, to speak about the benefits of trade liberalization, dispute settlement, and transparency as outstanding WTO achievements that had propelled global growth.

Founded twenty-five years ago as the successor to GATT, WTO is at a point in its evolution where it is felt that its mandate needs serious examination and reform. This internal process has reached a critical point, a situation that will undoubtedly color the 2020 Ministerials. WTO members are developing recommendations for updating the organization's mandate, as a result of new membership in recent years by major emerging economies, entailing challenges to WTO founding objectives.

The most immediate challenge is to the WTO Appeals Court, which judges conflicts over tariffs, subsidies, intellectual property and other disputes between members. If the Court is unable to continue its dispute resolution mandate, WTO will lose one of its most vital basic functions and strengths.

Given the importance to both Kazakhstan and to the foreign investment community that AmCham represents, AmCham intends to continue its enquiry into Kazakhstan's WTO commitments and the current status of WTO itself as it prepares for MC12 in Nur-Sultan in June 2020.

October Council Session: Cybersecurity and Cybercrime – A Challenge for the 21st Century

Prime Minister Mamin demonstrated the seriousness of Cybersecurity for the Government by convening virtually the entire Cabinet at the October Council meeting. The topic is also critical for AmCham members and the business community following the disruptive *Wannacry* cyberattack two years ago on a number of leading foreign companies in Kazakhstan. Although the Government has not acknowledged cyberattacks on its own systems, it is especially vulnerable through its widespread use of pirated software and other unlicensed technology. The new *Digital Kazakhstan* initiative also increases the country's vulnerability to cyberthreats.

The importance of intellectual property protection was stressed, along with recent changes to the legal and regulatory systems governing cybersecurity for commercial purposes, government protection (communications confidentiality and malicious attacks from other states), and general protection of the populace (identify theft, financial fraud). Cybercrime and cybersecurity are rapidly moving targets and cybercriminals are often ahead of the curve.

AmCham Speakers were from the technology sector – Microsoft, Ericsson, Honeywell, and the financial sector – Citibank and Mastercard. Honeywell brought their President for Russia and the Customs Union from Moscow, Microsoft brought their Corporate Affairs Director from Moscow, and Ericsson was represented by their CEO in Kazakhstan. Mastercard brought its Country Director from Warsaw, and Citibank was represented by its CEO in Kazakhstan.

All the above companies have sophisticated cybersecurity strategies and cyber units to protect their technology and banking services, services that are in high demand these days. Ericsson, whose operations are at the cutting edge of 5G services, stressed the importance of cybersecurity for 5G, whose use will spread across critical sectors such as power generation and transmission, transport, banking, health, and industrial control systems carrying sensitive information and safety systems.

Honeywell stressed the importance of cybersecurity for the oil industry as part of a country's critical infrastructure and the need for continual staff training to ensure awareness of cyber vulnerabilities and risks. Microsoft discussed cloud computing and the company's strategy to update cybersecurity for all purposes. Citibank and Mastercard provided an overview of cybercrime threats to the banking and financial services industry and discussed their defensive strategies to protect customer and client data, and to prevent cyberfraud and identify theft. The Council's corporate speakers were approached afterwards by Ministers requesting meetings to discuss the future security of their communication and data systems.

November Council Session: Fair Competition: A Basic WTO and OECD Requirement

The November Council revisited a WTO commitment shared by OECD, to ensure Fair Competition, ie a level playing field, for trade and investment. At a 2018 Council session, Prime Minister Sagintayev asked AmCham to seek the support needed by Kazakhstan to reform its competition practices. AmCham turned to the OECD, which willingly designed a short-term competition program that has not yet been implemented.

OECD Senior Competition Expert Sabine Zigelski outlined three recommendations made by the OECD after a review of Kazakhstan's competition law and policy, chief among these the need for institutional independence of the competition authority and the need to enforce anti-monopoly legislation on state-owned enterprises. The competition authority is currently part of a Ministry, which places it in the position of following government directives, distorting competition in favor of SOEs, and discriminating against foreign businesses.

A noteworthy Guest Speaker attended the November Council at the invitation of the Canadian Embassy: *Stephane Dion*, a well-known Canadian public figure and politician, Most recently *Minister of Foreign Affairs for Canada*, Mr. Dion is now *Prime Minister Trudeau's Special Envoy to the European Union and Europe*.

Stephane Dion's presentation displayed a thorough knowledge of Kazakhstan's economy and its challenges. In particular he addressed the need to confront and eliminate corruption in order to foster a robust and healthy competitive environment that would enable Kazakhstan to develop to its full potential. He also stressed that non-competitive pricing causes inflation and places economic pressure on the population that can eventually lead to social unrest.

Discriminatory tax policy and other practices designed to favor local companies were discussed by other speakers, as was the need to privatize state-owned enterprises that act as monopolies, imposing discriminatory regulations and tender requirements on foreign companies. The Government's role in price regulation, resulting in discriminatory pricing for foreign investors while local businesses are allowed more liberal pricing was also raised, as was government procurement policy. Government procurement is seen by foreign investors as discriminatory, resulting in their lack of participation in the tender process and having a negative effect on the investment climate.



AMCHAM WORKING GROUP UPDATE

SEPTEMBER - DECEMBER 2019

Almaty Working Groups

Almaty Trade and Customs Working Group

November On 29 November, the Trade and Customs Almaty Working Group led by *Chairman Siddique Khan*, convened to discuss two topics – the inclusion of royalties into the customs value of goods and issues concerning the 'Virtual Warehouse.' Both topics were presented by Oxana Sirotina and Timur Makarov from Globalink logistics.

Of the two topics, the introduction of the Virtual Warehouse was the most important. This new regulation will enter into force on 1 January 2020, but has left the business community with little time to prepare. In response, the Working Group is drafting a letter to present to the Government early next year.

Almaty Human Resources Working Group Almaty

October On 9 October, the Human Resources Almaty Working Group chaired by *Anar Khasenov from PwC* included a presentation from *Denis Couturier of UCLA*, which focused on UCLA's extension programs for degree or non-degree certificate courses both in the US, online, and in Kazakhstan.

Afterwards, PwC led a presentation on developing 'safety culture' which proposes a shift in company policy from passive, reactionary methods to active measures that prevent future injuries and deaths. The presentation outlined incentives to re-enforce safety culture by motivating employees to engage in safe practices.

November On 19 November, the HR Working Group convened to hear *Polina Karelina from Nestle* introduce flexible work schedules with a focus on maternity leave. She presented four solutions allowing women to remain in their professions while caring for themselves during and after pregnancy through partial workdays, remote work, flexible hours, and sabbaticals. She also discussed the concerns about flexible schedules and how their implementation is beneficial for companies.

PwC's *Zhadyra Adambayeva* then presented general salary trends in Kazakhstan. These include a general decrease in benefits, gender-based disparities in salaries, and differences in bonuses between levels of management.

December On December 11th, the working group convened once more. *Dina Akhmetova from Air Astana*, began with a presentation on the airline's *Electronic Document Management System*. The second half of this meeting was a broader, general discussion led by the PwC team concerning updates to the website *enbek.kz*.

Almaty Healthcare Reform Working Group

October On 24 October, the Healthcare Reform Working Group chaired by *Ksenia Babushkina of EY* met to discuss updates on Kazakhstan's healthcare system. One issue was the small-scale implementation of a new 'Health Passport'. Preliminary shortcomings concerned regionalization of information management for medical records, creating difficulties for this system to fulfil its objective of becoming a nation-wide health passport. There were also discrepancies between the records and the patients' own information.

Almaty Corporate and Social Responsibility Working Group Almaty

November On 4 November, the Corporate Social Responsibility Working Group led by *Asad Shirinov of Coca-Cola* invited *Viktor Kovalenko from EY* to present *Social Return on Investment (SROI) Accounting*. The premise of SROI is that investing in social programs can be in the economic interests of a private company or companies. This translates into fewer expenditures toward health insurance and a measurable increase in productivity. With SROI accounting, companies can maximize their per-dollar returns from social investments while decreasing intangible or indirect losses.

Almaty Tax Working Group

October On 24 October, *Vera Kapatsina from Angels Niko Advisory* delivered a presentation on the types of taxes levied on foreign residents in Kazakhstan and on Kazakhstani citizens. This was followed by a presentation by *Karina Kalimzhanova and Gulsara Ryskeldinova from the Deloitte Tax and Law Department* on tax residency certificate issues. It outlined challenges faced by foreign workers in Kazakhstan due to conflicting inter-institutional standards.



Nur-Sultan Working Groups

Nur-Sultan Human Resources Working Group

October On 15 October, the Nur-Sultan Human Resources Working Group met in the EY office under Group Chairman *Damir Deminov, EY Senior HR Manager*. The Keynote Speaker was *Dr. Zoltan Buzady, Associate Professor of Management and Organization, Corvinus University of Budapest*. The speaker delivered a presentation on the theory of 'FLOW', a mental state in which a person is fully immersed in an activity: energized, focused, and fulfilled.

A testing process for leadership growth aimed at supporting FLOW in the workplace was also presented. The test offered an assessment of different leadership styles and their effect on an organization can be assessed (team spirit, company atmosphere, profitability etc.).

Nur-Sultan Trade and Customs Working Group

October On 15 October, the Nur-Sultan Trade and Customs Working Group met in the EY office under Group Chairman *Samat Karmys, EY Senior Associate*. The first speaker, *Kozhakhmet Iskakov, EY Trade and Customs Expert* spoke about customs risks that may arise when importing goods and seeking to control the customs value with recommendations for avoiding undesirable consequences.

Sarmat Karmys delivered a presentation on customs risks when changing the distribution model of a business to that of your own company. *Ms. Dossymkhanova, Deloitte Manager, Tax and Legal Department*, outlined anticipated developments in customs legislation: taxes, temporary storage of goods, customs control forms, and appeal procedures.



**1 JANUARY - 31 MARCH
HURRY TO BOOK YOUR CONFERENCE!**

**С 1 ЯНВАРЯ ПО 31 МАРТА
УСПЕЙТЕ ПРИОБРЕСТИ
КОНФЕРЕНЦ-ПАКЕТЫ ПО СПЕЦИАЛЬНЫМ ЦЕНАМ!**



**20% DISCOUNT
FOR CONFERENCE
PACKAGE**

**20% СКИДКА
НА КОНФЕРЕНЦ-
ПАКЕТЫ**

FULL DAY / ПОЛНЫЙ ДЕНЬ

~~**21.400 KZT**~~
per person / на человека

17.120 KZT
per person / на человека

HALF DAY / ПОЛДНЯ

~~**18.100 KZT**~~
per person / на человека

14.480 KZT
per person / на человека

30% DISCOUNT FOR ROOM RENTAL*
30% СКИДКА НА АРЕНДУ ЗАЛОВ*

BOOK CONFERENCE PACKAGE FOR 2 DAYS AND GET COMPLIMENTARY
WELCOME COFFEE BREAK: TEA, COFFEE, JUICE, COOKIES AND FRUITS**

БЕСПЛАТНЫЙ ПРИВЕТСТВЕННЫЙ КОФЕ-БРЕЙК (ЧАЙ, КОФЕ, СОКИ, ФРУКТЫ
И ПЕЧЕНЬЕ) ПРИ БРОНИРОВАНИИ 2-Х ДНЕЙ**

*Prices include VAT and are subject to 10% service charge. / *Цены включают НДС, 10% сервисного сбора будут добавлены к итоговой сумме счета.
**Number of guests should be from 10 to 50 / **Минимальное количество гостей от 10 до 50



ATYRAU
OIL&GAS KAZAKHSTAN

19th North Caspian Regional Atyrau Oil&Gas Exhibition

8-10 April 2020

Atyrau, Kazakhstan

Find out more at

www.oil-gas.kz





AMERICAN CHAMBER OF COMMERCE IN KAZAKHSTAN

MEMBERSHIP APPLICATION

ABOUT AMCHAM

Registered in Kazakhstan as a non-profit organization in March of 1999 with 36 charter members, the American Chamber of Commerce in Kazakhstan currently represents over 200 member companies including US, multinational, and local businesses in 30 industry sectors. Their collective investment in Kazakhstan's economy is several billion USD. The American Chamber in Kazakhstan is a member of the US American Chamber of Commerce in Washington D.C. and has working relationships with many regional business associations.

BENEFITS OF MEMBERSHIP

- ✓ AmCham members participate in an organization existing solely to serve members
- ✓ AmCham actively advocates for reform of the business environment with Kazakhstan Government at senior levels
- ✓ AmCham Members may attend 19 Working Groups in 5 cities plus Inter-Ministerial Working Groups
- ✓ Monthly speaker luncheons with senior government and business leaders are reserved for AmCham members
- ✓ Seminars, conferences, and monthly social networking events are organized for AmCham members
- ✓ AmCham membership contact lists are available exclusively to AmCham members
- ✓ Economic, political, legal, social, and business development information is distributed to members
- ✓ Member companies provide exclusive discounts on products and services to other AmCham members
- ✓ Access to the Members' Only section on the AmCham Website
- ✓ Publishing opportunities are available in *Investors' Voice*, the *Annual Membership Directory*, and Special Publications

MEMBERSHIP APPLICATION

Company Name:

Industry Area:

CEO Name, Signature, Email:

Contact Individual:

Title(s):

Address:

Tel.: Fax: E-mail:

Please include us in the following Working Groups:

Almaty (7)

- | | |
|--|--|
| ☐ Foreign Investment | ☐ Healthcare Reform |
| ☐ Human Resources | ☐ Trade and Customs |
| ☐ Tax | |
| ☐ Technology and Innovation | |
| ☐ Corporate Social Responsibility | |

Atyrau (4)

- | |
|--|
| ☐ Tax |
| ☐ Human Resources |
| ☐ Trade and Customs |
| ☐ Corporate Social Responsibility |

Aktau (3)

- | |
|--|
| ☐ Human Resources |
| ☐ Tax |
| ☐ Trade and Customs |

Nur-Sultan (4)

- | |
|---|
| ☐ Foreign Investment |
| ☐ Tax |
| ☐ Trade and Customs |
| ☐ Human Resources |

Shymkent (1)

- | |
|---|
| ☐ Foreign Investment |
|---|

AMCHAM WORKING GROUPS

Working Groups made up of representatives from Amcham member companies provide comment, discussion and submission of positions and represent the united interests of the business community in Kazakhstan by identifying challenges faced by investors and proactively addressing them. Each group meets regularly, providing a forum for networking and the exchange of information. Groups are formed on an as-needed basis at the request of the AmCham membership.

GOVERNANCE

The AmCham is governed by a Board of Directors elected annually from and by the membership. Directors currently and in the past have included individuals from the following company members:

AES	HSBC
AIG Insurance	Hyatt Hotel
Baker & McKenzie	Honeywell
BASF Central Asia	Intercontinental Hotel
BG Group	KIMEP
Bracewell and Giuliani	KPMG
Capital Bank	LeBoeuf, Lamb, Greene
Chevron	Nestle
Citibank	Philip Morris Kazakhstan
Conoco Phillips	Philips Kazakhstan
Coca-Cola	PricewaterhouseCoopers
Dechert	Procter & Gamble
Deloitte	Raytheon
EBRD	Scot Holland CBRE
Ernst & Young	Tengizchevroil
GE International	Visor Capital
Halliburton	White & Case

OFFICE

Rixos Almaty Hotel Office Tower, 8th floor
Almaty Kazakhstan
Tel.: +7 (727) 330 92 50
www.amcham.kz

Doris Bradbury
Executive Director
Doris.Bradbury@amcham.kz

Rimma Kazhemyakina
Finance Director
Rimma.Kazhemyakina@amcham.kz

Dean Rodan
Publications / Working Groups Coordinator
Dean.Rodan@amcham.kz

Anar Zholdoshbek Kyzy
Publications / Communications Coordinator
Anar.Zholdoshbek.kyzy@amcham.kz

Akmaral Bekzhunissova
Government Relations Coordinator
Akmaral.Bekzhunissova@amcham.kz

Togzhan Smagulova
Events / Working Groups Coordinator
Togzhan.Smagulova@amcham.kz

Aigul Sauranova
Accountant
Aigul.Sauranova@amcham.kz

Zharkynay Ospan
Receptionist / Assistant
Info@amcham.kz

REGIONAL REPRESENTATIVES

Bela Ferenczi
CEO General Electric
Resident Representative, Astana
Bela.Ferenczi@ge.com

Dorin Baru
CEO OMV Petrom
Resident Representative, Aktau
Dorin.Baru@omv.com

Wojciech Halat
CEO HeidelbergCement
Resident Representative, Shymkent
Wojciech.Halat@heidelbergcement.kz

MEMBERSHIP CATEGORIES AND ANNUAL FEES

Corporate A	(Worldwide revenues in excess of 100 million USD)	\$5,000 USD
Corporate B	(Worldwide revenues between 2-100 million USD)	\$3,800 USD
Corporate C	(Worldwide revenues not exceeding 2 million USD)	\$2,700 USD
Non-Profit		\$1,500 USD
Individual**		\$500 USD

***Individual memberships are available only under special circumstances for persons not associated with a company.*

Corporate membership entitles a company to delegate 3 individuals as AmCham voting members. The number of persons from each company participating in working groups, forums, and business roundtables is usually not limited.

All applications for membership must be approved by the Board of Directors of the American Chamber of Commerce in Kazakhstan. For further information about membership benefits, the application process, or Investors' Voice magazine, please contact: info@amcham.kz



Business



Новый уровень контроля устройств

Управляйте оборудованием через мобильную сеть
и контролируйте установленные в них SIM-карты



PEPSICO

