CYBER TRENDS AND INSIGHTS

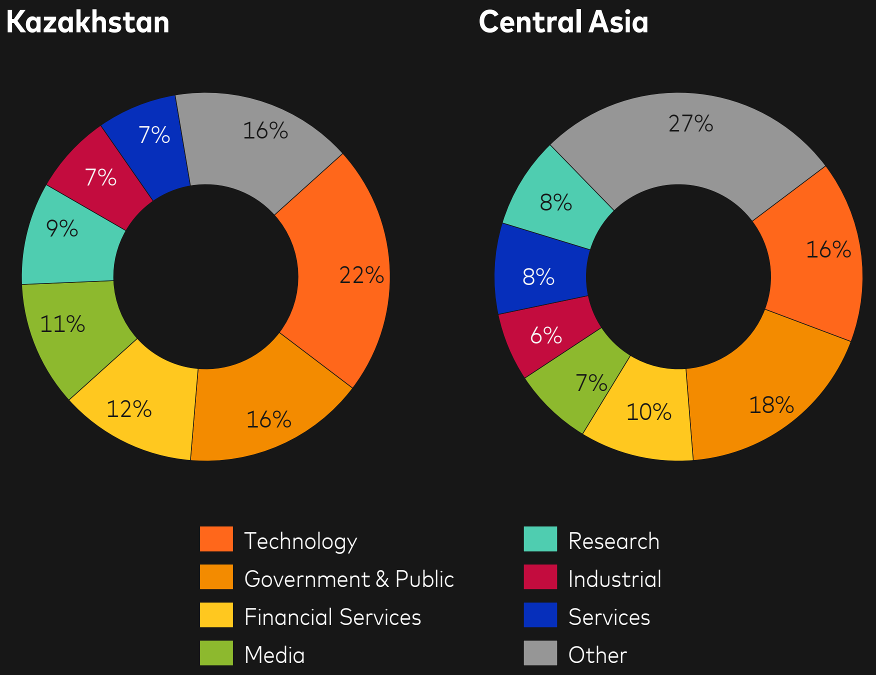
# Cybersecurity Landscape in Kazakhstan & Global Best Practices

March 2023

CYBER THREAT LANDSCAPE IN KAZAKHSTAN

# In Kazakhstan and Central Asia, Government & Public and Financial Services are targets of almost a third of all cyber events

## Cyber events per industry


Kazakhstan

Central Asia

## Most popular Assets, Actors and TTP

### *Assets*

35%

of events targeting Intellectual Property or Business Systems

**Central Asia average: 44%**

### *Actors*

65%

of events were attributed to politically-motivated attackers

**Central Asia average: 72%**

### *TTP*

54%

of attacks were performed through malware / ransomware or DDoS

**Central Asia average: 44%**

Source: Mastercard Cyber Insights Data
Based on data for the time period 1st October 2022 – 26th March 2023

# REGULATORY FRAMEWORK

- The Cybersecurity was approved by the Resolution of the Government of the Republic of Kazakhstan No. 407 of 30 June 2017. The Cybersecurity Concept was developed for the period of 2017 to 2022. (https://adilet.zan.kz/kaz/docs/P1700000407#z10 )

- The Law of the Republic of Kazakhstan of 21 May 2013 No. 94-V on Personal Data and its Protection ('the Personal Data Law') provides the principles on the collection and processing of personal data and includes broad requirements for data localization. (https://adilet.zan.kz/eng/docs/Z1300000094)

- In July 2020, The Law on Amendments and Additions to Some Legislative Acts of the Republic of Kazakhstan on the Regulation of Digital Technologies ('the Amendment Law') was introduced. (https://adilet.zan.kz/kaz/docs/Z2000000347)

- This Amendmend has significantly extended data protection obligations for organizations processing personal data.

- Other information security related regulations:
  - Uniform requirements in the field of information and communication technologies and information security
  - Rules for certification of the information system, the "e-government" information and communication platform, the Internet resource of a state body for compliance with information security requirements
  - Rules for confirming the conformity of information systems, hardware, software and hardware and software tools (products), technical means of protecting information with information security requirements

# Essential practices to enhance cybersecurity posture

## Establish a non-negotiable cybersecurity culture

**Strengthening the awareness and training program**, thus ensuring collaborators are defenders of cybersecurity by eliminating bad habits that negatively affect the organization's security posture. Invest in user training.

## Establish and know your cyber perimeter

In today's networks the **limits or perimeter of the network are not drawn and no longer exist**, or single-entry points defined. This panorama obliges organizations to have identified its borders and limits in order to identify the associated risks and implement the appropriate controls such as **network access, firewall, IPS, IDS**.

## Collect, monitor, and analyze information to build cyber intelligence

Build a **management program for the management, intelligence, and investigation of cybersecurity incidents** to minimize the adverse impacts on your operations by carrying out identification, analysis, treatment, response, and containment activities, through the correct articulation of the attention and response teams.

## Build a third-party risk management program

Establish a program to allow you to **manage and monitor your critical third parties to prevent their risk becoming your risk**.

## Strengthening your controls against malware

Implementing controls for **monitoring users' behavior, network content scanning & filtering, secure browsing, and powerful awareness, culture, and training programs** allow you to protect against these attacks.

## Manage change management and hardening programs

Incorrect settings are a gateway for attackers. Building a **robust change management program** allows organizations to manage and review changes before they are converted into a door for attackers or put the organization at risk.

## Patch apps and systems

The management of patches and vulnerabilities in an organization is one of the main components in managing and administering risk; in fact, the management of patches and vulnerabilities is the center of **cyber resilience and hygiene**.

# Statement of Confidentiality and Disclaimer

©2023 Mastercard. All third-party product names and trademarks belong to their respective owners. The information provided herein is strictly confidential. It is intended to be used internally within your organization and cannot be distributed or shared with any other third party, without MasterCard's prior approval. The parties acknowledge that other terms and conditions are also anticipated to be considered.

Information in this presentation or in any report or deliverable provided by MasterCard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both MasterCard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent. The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. MasterCard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation.