МОНГОЛ УЛСЫН ЗАСГИЙН ГАЗАР
ЭРҮҮЛ МЭНДИЙН ЯАМ

МОНГОЛ УЛСЫН ЗАСГИЙН ГАЗАР
ЦАХИМ ХӨГЖИЛ, ХАРИЛЦАА ХОЛБООНЫ ЯАМ

unicef
НҮБ-ын Хүүхдийн Сан

ЦАХИМ ЭРҮҮЛ МЭНД

Гантөмөр Гантуяа

Кибер халдлага зөрчилтэй тэмцэх нийтийн төвийн Кибер халдлагаас урьдчилан сэргийлэх газрын дарга

Cyber Security in Healthcare Sector

GANTUYA GANTUMUR
HEAD OF CYBER ATTACK PREVENTION DEPARTMENT

01

Overview of Information Security in the Healthcare Sector

02

Common Vulnerabilities and Risks

03

Regulatory Framework and Compliance Requirements

04

Challenges


Overview of Information Security in the Healthcare Sector

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

THE IMPACT OF CYBERSECURITY ON THE GLOBAL ECONOMY

In 2024	9.2 trillion
Monthly	766 billion
Weekly	178.8 billion
Daily	25.5 billion
Hourly	1 1,06 billion
Minutely	17.7 million
Secondly	295,7 thousand

As of 2024, the economic losses from cybercrime in US dollars

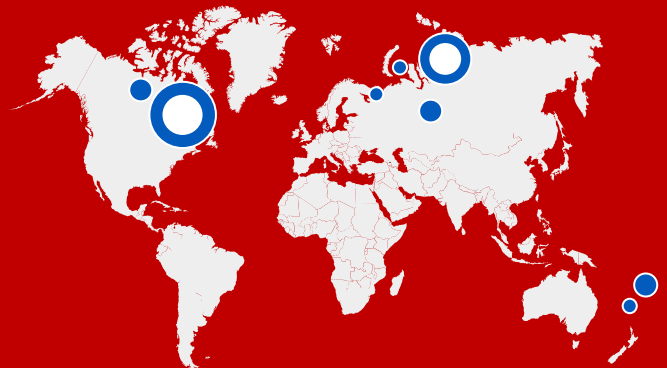
Cost to the global economy

2024 он	9,200,000,000,000$
2025 он	10,500,000,000,000$

Ransomware attack

71% of global businesses felt the impact of ransomware trends
average cost of $896,000.

U.S. Agency for International Development (USAID) report:

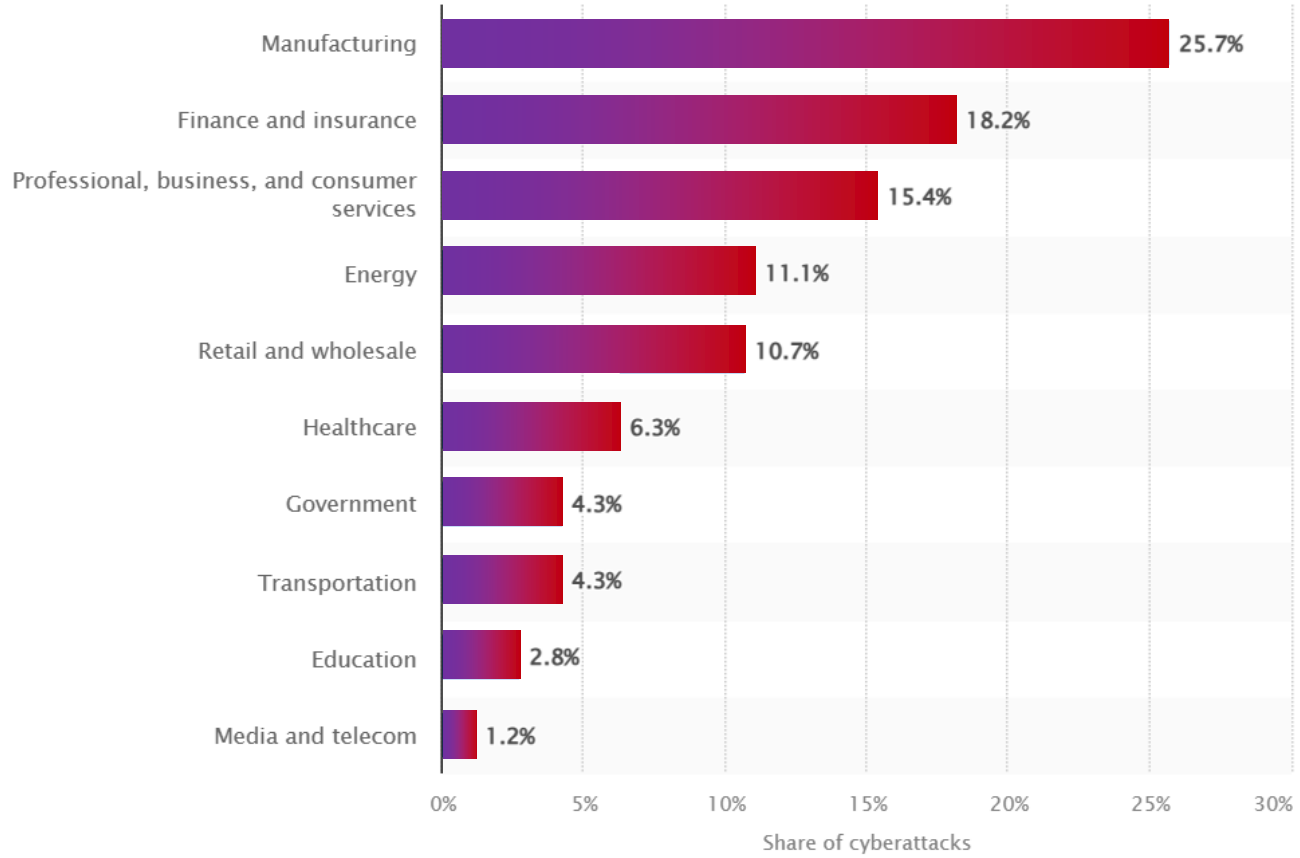


There are around 2,220 cyberattacks each day, and that equates to more than 800,000 attacks each year, according to Security Magazine.

According to one estimate, the global cost of cybercrime is estimated to top $8 trillion in 2023. This figure is larger than the national economies of all but two countries—the United States and the People's Republic of China. And cybercrime is expected to continue to grow unabated over the coming years, with projections as high as $23.84 trillion by 2027.

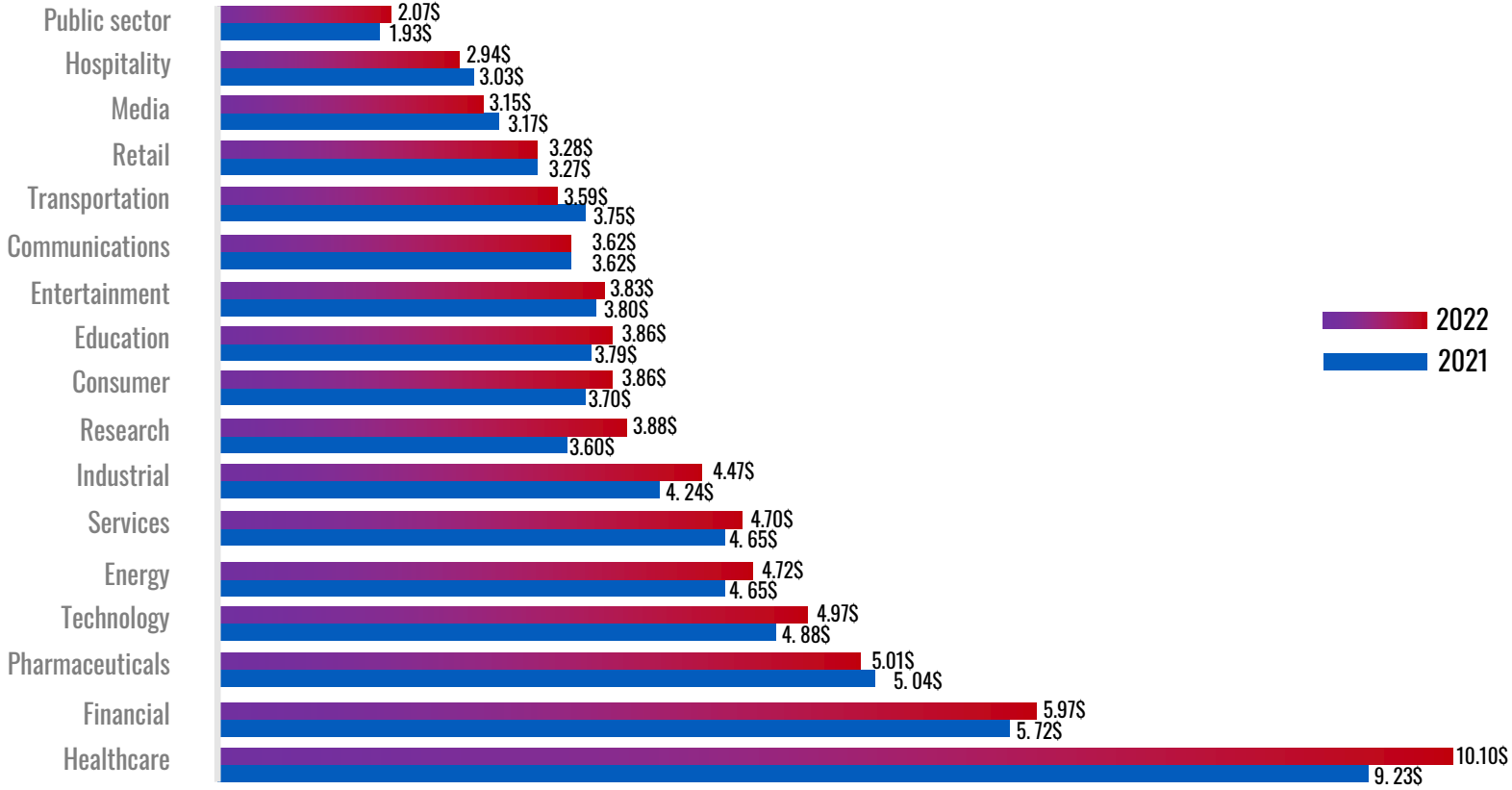
https://gia.gov.mn/49/item/643
https://www.usaid.gov/digital-development/cybersecurity/economic-growth-briefer#:~:text=cybersecurity%20as%20the%20single%20greatest,top%20%248%20trillion%20in%202023.
2023 was a big year for cybercrime – here's how we can make our systems safer | World Economic Forum (weforum.org)

Distribution of cyberattacks across worldwide industries in 2023



КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

AVERAGE COST OF DATA BREACHES WORLDWIDE BY INDUSTRY, 2022 vs 2021

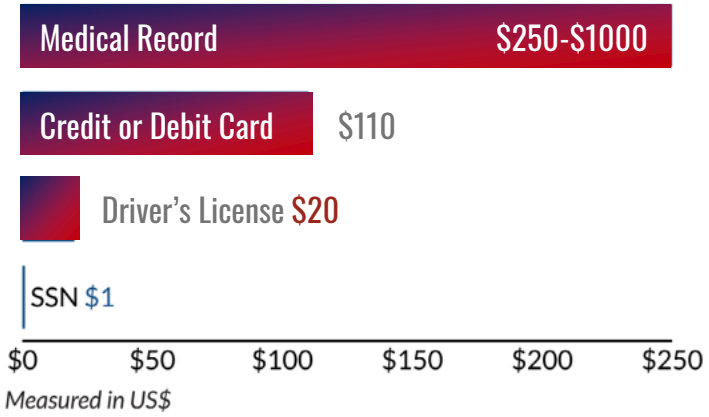


КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

Reasons why healthcare is the biggest target for cyberattacks

1. Private patient information is worth a lot of money to attackers

FIGURE 1 Cost per piece of personal information on the Dark Web



Reasons why healthcare is the biggest target for cyberattacks

2. Healthcare staff aren't educated on online risks

According to the report, **34%** of U.S. healthcare workers are unaware of their company's cybersecurity policy while **14%** are aware of their company's policy but never read it.

One in four U.S. healthcare workers have never received cybersecurity training from their employer, according to a new report by Kaspersky

Another 19% believe there is no reason to receive cybersecurity training at work

Reasons why healthcare is the biggest target for cyberattacks

73%

USE VPN CONNECTIONS

46%

MULTI FACTOR AUTHENTICATION

18%

DEVICE RISK POSTURE CHECK

18%

ZERO TRUST NETWORK ACCESS

3. Staff need to access data remotely, opening up more opportunities for attack

- **60%** of remote workers use unsecured personal devices to access their employer's network.
- Only **17%** reported limiting remote access to corporate laptops.
- Ransomware attacks have surged by **20%** since the remote work shift.

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

Reasons why healthcare is the biggest target for cyberattacks

4. Use of Outdated Technology

5 SECURITY RISKS

1. Security Vulnerabilities
2. Data Breaches
3. Integration Challenges
4. Compliance Risks /HIPAA/
5. Outdated security protocols

Reasons why healthcare is the biggest target for cyberattacks

5. NOT FOLLOWING SECURE CODING STANDARDS

Vulnerabilities in poorly coded software can be exploited by cybercriminals to gain unauthorized access to sensitive patient data, such as medical records, treatment histories, and personal information.

Healthcare organizations are subject to stringent regulatory requirements regarding the security and privacy of patient information, such as HIPAA in the United States or GDPR in the European Union.

Exploitation of vulnerabilities in insecure code can result in system downtime, service disruptions, or even ransomware attacks.

Reasons why healthcare is the biggest target for cyberattacks

6. Healthcare information needs to be open and shareable

CYBERSECURITY

Integrity | Confidentiality | Availability

System for Health Data Collection and Transmission

An authentication system

Access rights policy


Common Vulnerabilities and
Risks

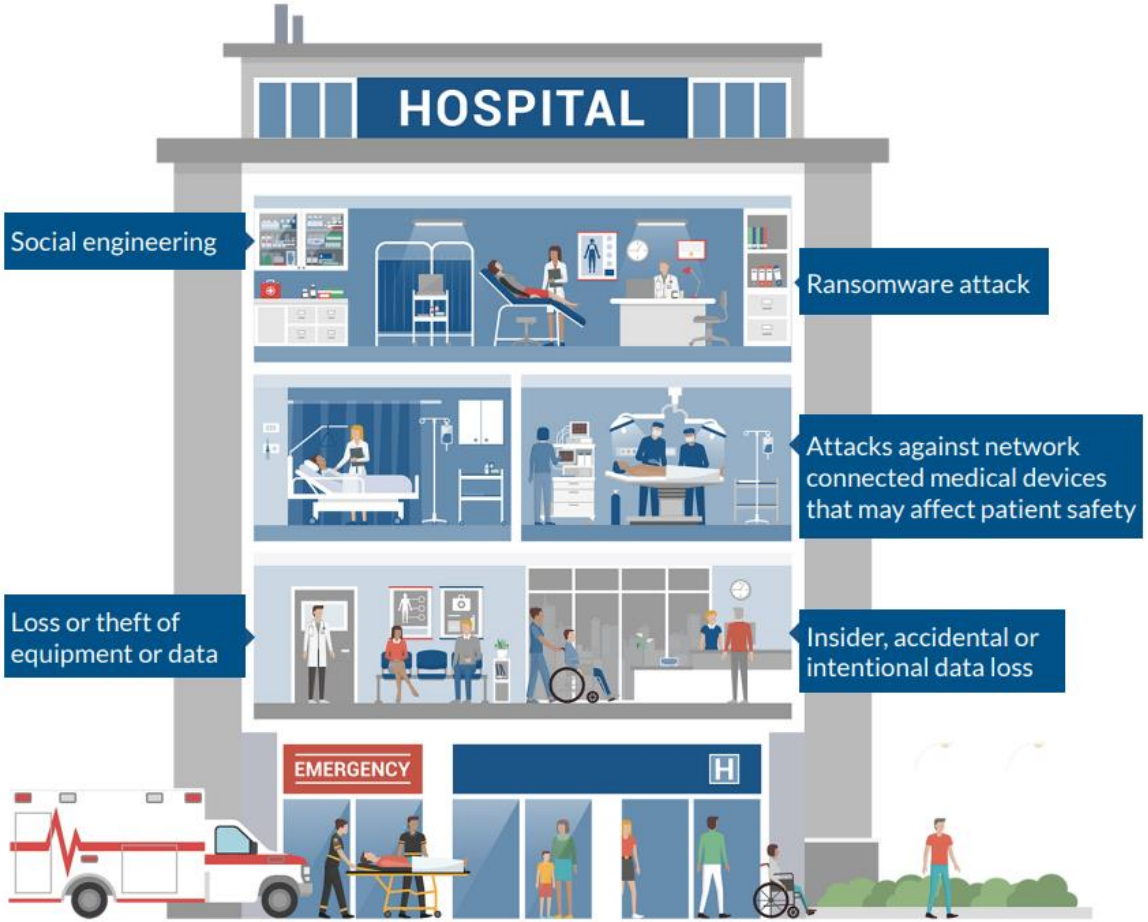
DATA BREACHES

TOP-10 healthcare data breaches of all time

Rank	Company	Date	No. of People Affected
1.	Anthem Blue Cross	January 2015	78.8 Million
2.	American Medical Collection Agency	March 2019	26.1 Million
3.	Brazil Ministry of Health	November 2020	16+ Million
4.	Premera Blue Cross	January 2015	11+ Million
5.	Excellus BlueCross BlueShield	September 2015	10+ Million
6.	Managed Care of North America	March 2023	8.9 Million
7.	UK National Health Service (NHS)	July 2011	8.6 Million
8.	PharMerica	March 2023	5.8 Million
9.	MedicareSupplement.com	May 2019	5 Million
10.	TRICARE	September 2011	4.9 Million

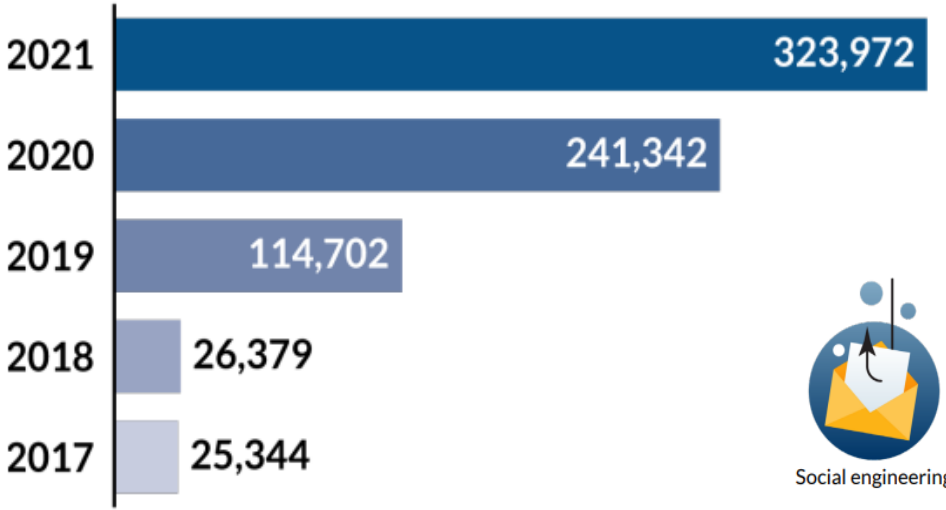
safetydetectives.com

Top 5 threats facing the healthcare sector

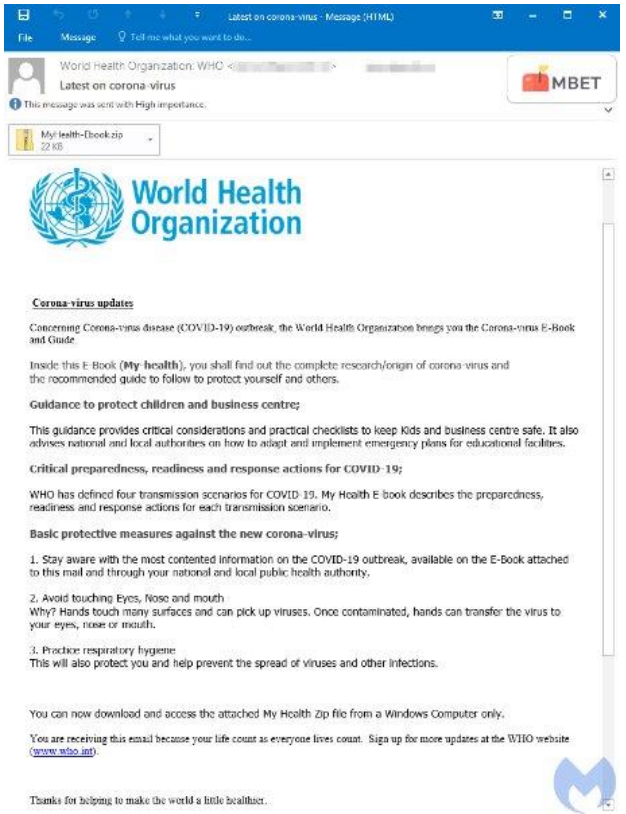


Social engineering

Number of phishing/vishing/smishing/ pharming victims reported to the FBI Internet Crime Complaint (IC3), 2017-2021



Social engineering



Latest on corona-virus - Message (HTML)

File Message Tell me what you want to do...

World Health Organization: WHO <

Latest on corona-virus

This message was sent with High importance.

MBET

My Health-Ebook.zip
22 KB

World Health Organization

Corona-virus updates

Concerning Corona-virus disease (COVID-19) outbreak, the World Health Organization beegs you the Corona-virus E-Book and Guide

Inside this E-Book (**My health**), you shall find out the complete research/origin of corona-virus and the recommended guide to follow to protect yourself and others.

Guidance to protect children and business centre;

This guidance provides critical considerations and practical checklists to keep kids and business centre safe. It also advises national and local authorities on how to adapt and implement emergency plans for educational facilities.

Critical preparedness, readiness and response actions for COVID-19;

WHO has defined four transmission scenarios for COVID-19. My Health E book describes the preparedness, readiness and response actions for each transmission scenario.

Basic protective measures against the new corona-virus;

1. Stay aware with the most contented information on the COVID-19 outbreak, available on the E-Book attached to this mail and through your national and local public health authority.

2. Avoid touching Eyes, Nose and mouth
Why? Hands touch many surfaces and can pick up viruses. Once contaminated, hands can transfer the virus to your eyes, nose or mouth.

3. Practice respiratory hygiene
This will also protect you and help prevent the spread of viruses and other infections.

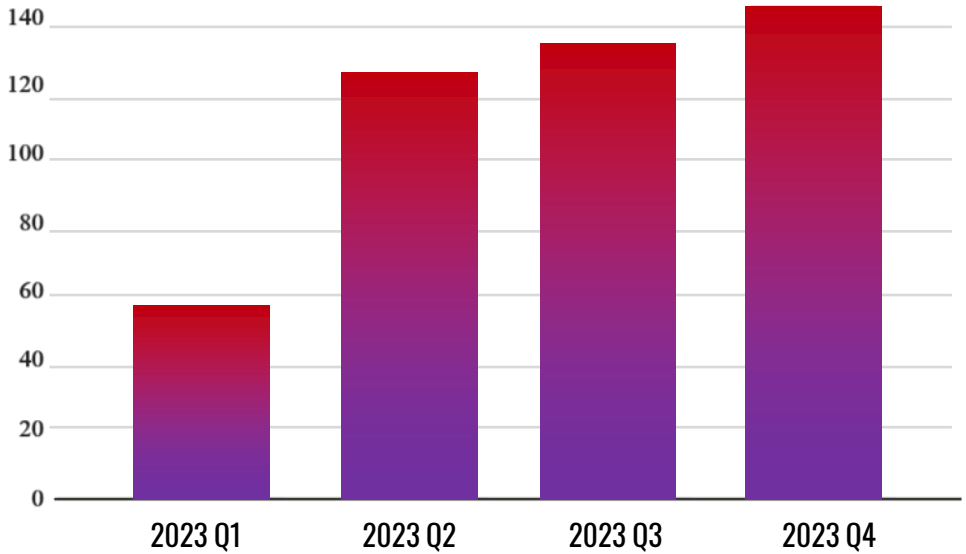
You can now download and access the attached My Health Zip file from a Windows Computer only.

You are receiving this email because your life count as everyone lives count. Sign up for more updates at the WHO website (www.who.int).

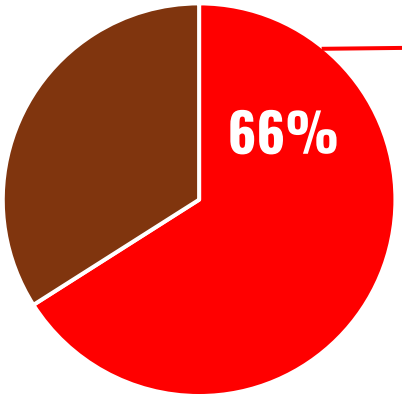
Thanks for helping to make the world a little healthier.

Threat: Ransomware Attack

Ransomware Attacks Against Healthcare



Organizations affected by ransomware in 2021



66% of healthcare organizations affected by ransomware attack in 2021

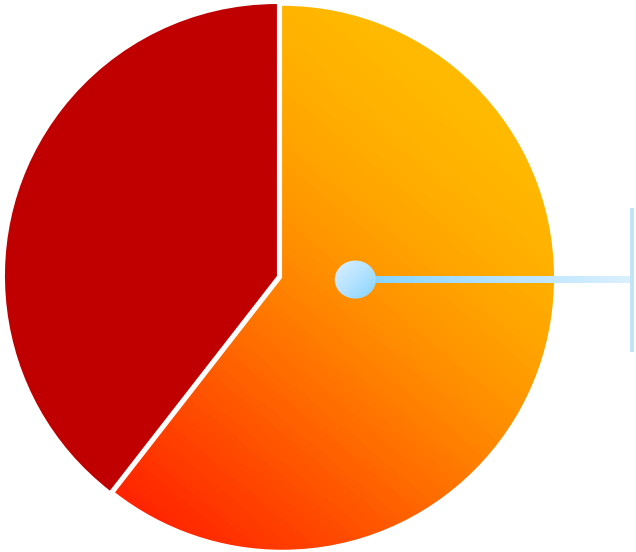
Ransomware attacks

https://405d.hhs.gov/Documents/HICP-Main-508.pdf

Threat: Attacks Against Network Connected Medical Devices

Patients are at great risk because an attack has shut down heart monitors, including ones being used in surgery and other procedures. Doctors are now distracted, quality of patient care has suffered, and patients' health is at risk.

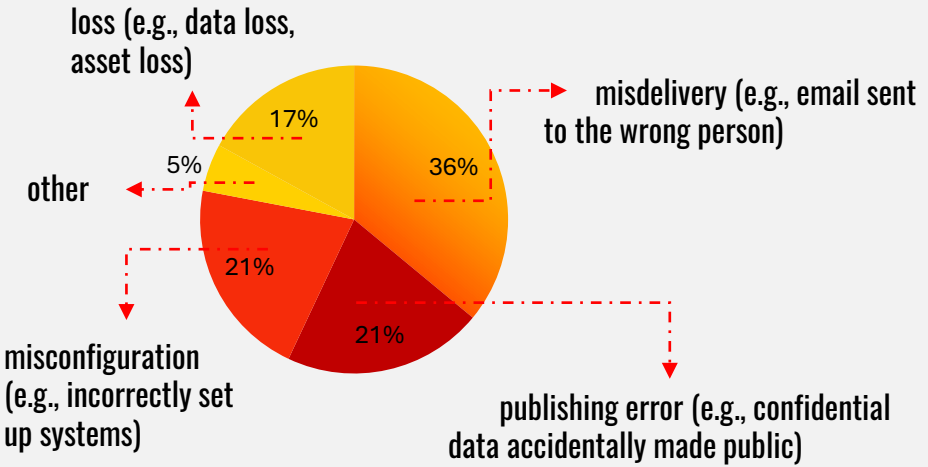
Internet of Things (IoT) vulnerabilities



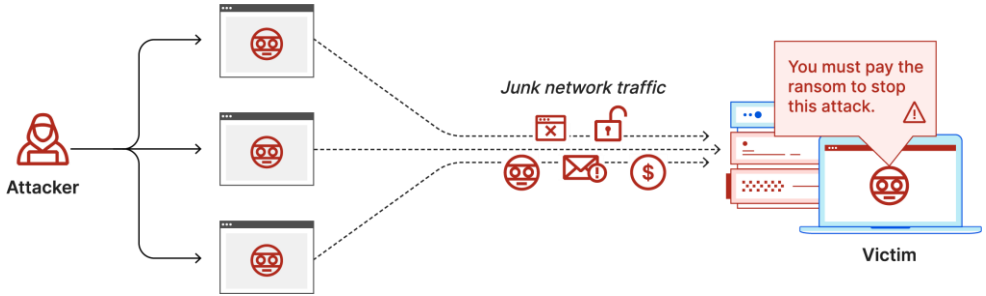
Data shows that **53%** of connected medical devices and other IoT devices in hospitals have a known critical vulnerability.

Threat: Loss or Theft of Equipment or Data

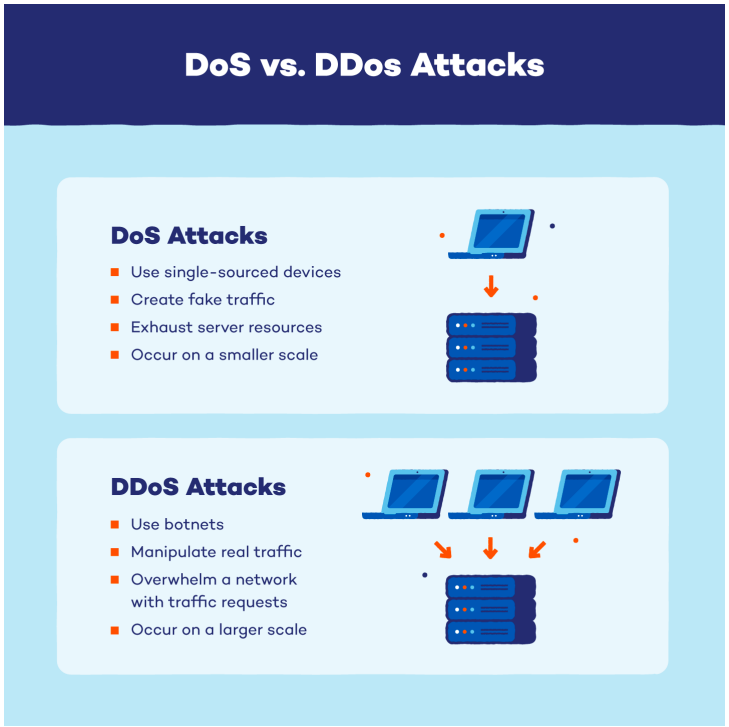
An employee with access to patient records begins to print extra copies of patient records that include a significant amount of sensitive information such as PHI. They then take the copies and sell them on the dark web.



DoS, DDoS халдлага



- Үйлчилгээ тасалдах
- Жинхэнэ хэрэглэгчид системд хандах боломжгүй болох
- Байгууллагын нэр хүнд унах, хэрэглэгчдээ алдах



DoS, DDoS attack

Without insulin they’re going to die

Ronda Miller, 54, said she and her husband rely on a discount card to afford his insulin — he has Type 2 diabetes and congestive heart failure. But when she tried to pick up his medication at her pharmacy in Deadwood, South Dakota, on Feb. 22, the card could not be processed. Without it, the medications would cost hundreds of dollars.


Regulatory Framework and
Compliance Requirements

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

USA

Regulatory Framework and Compliance Requirements	Scope of the law
Health Insurance Portability and Accountability Act (HIPAA) - 1996	HIPAA sets the national standards for the protection of sensitive patient health information. It includes the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.
Health Information Technology for Economic and Clinical Health Act (HITECH Act) - 2009	HITECH Act expanded HIPAA's privacy and security provisions and introduced additional requirements related to electronic health records (EHRs) and health information technology.
HITECH Omnibus Rule - 2009	This rule modified certain HIPAA provisions and extended the requirements to business associates, including subcontractors, that handle protected health information (PHI).
Health Information Exchange (HIE) - 2016	Various state laws and regulations govern health information exchange initiatives, promoting the secure sharing of electronic health information among healthcare providers.
Patient Protection and Affordable Care Act (ACA) - 2010	ACA includes provisions related to healthcare data and privacy, such as requirements for health insurance marketplaces and transparency in healthcare pricing and quality.
Federal Trade Commission (FTC) Act	The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC has authority to enforce privacy and data security requirements for non-healthcare-specific entities, such as certain vendors and businesses that handle consumer health data.
State Data Breach Notification Laws 2002 - 2024	Many states have enacted laws requiring organizations to notify individuals and regulators in the event of a data breach involving personal information, including health information.
Electronic Communications Privacy Act (ECPA) - 1986	ECPA governs the interception of electronic communications and includes provisions relevant to the privacy and security of electronic health information.
Genetic Information Nondiscrimination Act (GINA) - 2008	GINA prohibits the use of genetic information in health insurance and employment decisions and includes protections for genetic privacy.

Монгол Улс

8.4
HEALTHCARE LAW OF MONGOLIA

8.4.Эрүүл мэндийн мэдээллийг цуглуулах, боловсруулах, ашиглах, хадгалах, аюулгүй байдлыг хангах журмыг эрүүл мэндийн асуудал эрхэлсэн төрийн захиргааны төв байгууллага, цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагатай хамтран боловсруулж Засгийн газар батална.

19.1, 19.2
CYBERSECURITY LAW OF MONGOLIA

19.1.Онц чухал мэдээллийн дэд бүтэцтэй байгууллагад дараах чиглэлээр үйл ажиллагаа эрхэлдэг байгууллага хамаарна:

19.1.3.хоёр, гуравдугаар шатлалын эрүүл мэндийн байгууллага;

19.1.4.хүн, малын гоц халдварт өвчин судлах лаборатори;

19.1.5.эм, химийн хорт болон аюултай бодис үйлдвэрлэгч;

318, 319
PERSONAL DATA PROTECTION LAW OF MONGOLIA

5.1.Мэдээлэл цуглуулах, боловсруулах, ашиглахад дараах зарчмыг баримтална:

5.1.1.хүний эрх, эрх чөлөөг зөрчихгүй байх;

5.1.2.хүний эрх, хууль ёсны ашиг сонирхлыг хүндэтгэх;

5.1.3.ялгаварлан гадуурхахгүй байх;

5.1.4.мэдээллийг хуульд заасан үндэслэлээр, эсхүл мэдээллийн эзний зөвшөөрлийн дагуу цуглуулах, боловсруулах, ашиглах;

5.1.5.мэдээллийн аюулгүй байдлыг хангах;

5.1.6.мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг алдагдуулахгүй байх.

207
GOVERNMENT REGULATIONS

Хоёр, гуравдугаар шатлалын эрүүл мэндийн байгууллага (Лавлагаа шатны эрүүл мэндийн байгууллага болон Тусгай мэргэжлийн төв)

54

114.	Хүн, малын гоц халдварт өвчин судлах лаборатори	Зоонозын өвчин судлалын үндэсний төв	117.	Эм, химийн хорт болон аюултай бодис үйлдвэрлэгч байгууллага	Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын газар
115.		Халдварт өвчин судлалын үндэсний төв	118.		Хүний эм, эмнэлгийн хэрэгсэл, багаж, тоног төхөөрөмж, протез үйлдвэрлэх, худалдах, импортлох тусгай зөвшөөрөл бүхий байгууллагууд
116.		Нийслэлийн зоонозын өвчин судлалын төв	119.		Тэсэрч дэлбэрэхээс бусад химийн хорт болон аюултай бодис үйлдвэрлэх тусгай зөвшөөрөл бүхий байгууллагууд

Хоёр.Үндэсний төвийн чиг үүрэг, үйл ажиллагаа

318, 319
GOVERNMENT REGULATIONS

2.2.2.онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээд болон төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллагын мэдээллийн системд чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэх;

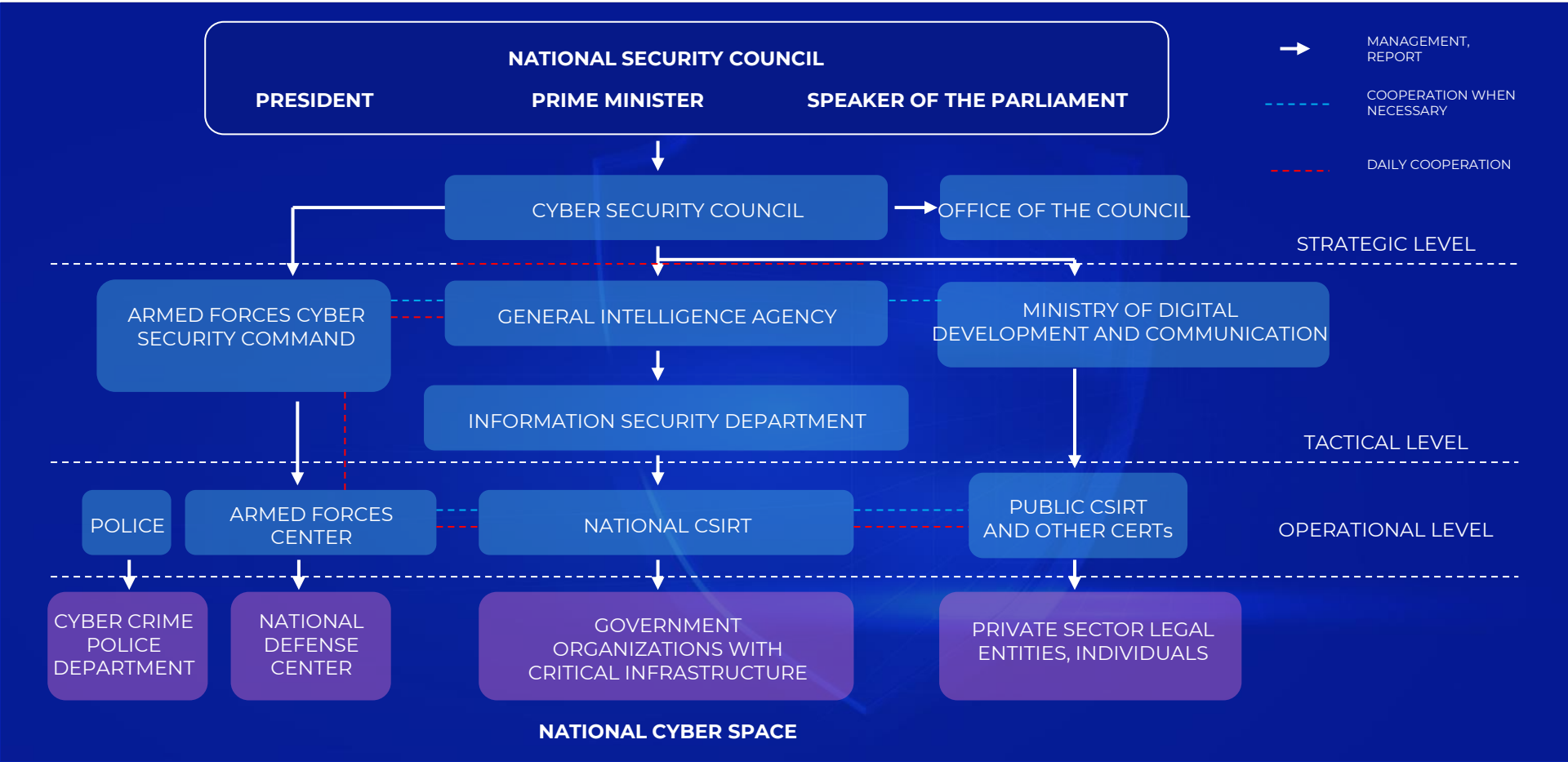
Хоёр.Нийтийн төвийн чиг үүрэг, үйл ажиллагааны чиглэл

2.2.1.иргэн, хуулийн этгээд, онц чухал мэдээллийн дэд бүтэцтэй хувийн хэвшлийн байгууллагын мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдалд зөвлөмж өгөх;

Article 19 of the Law on Cyber Security. An organization with critical information infrastructure:
19.2.1.кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах;
19.2.2.кибер халдлага, зөрчлийн үед дагаж мөрдөх төлөвлөгөөг баталж хэрэгжүүлэх;
19.2.3.мэдээллийн аюулгүй байдлыг хангах талаар стандартыг нэвтрүүлэх;
19.2.4.кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтантай байх;
19.2.5.кибер аюулгүй байдлын эрсдэлийн үнэлгээг жил тутамд, эсхүл мэдээллийн систем, мэдээллийн сүлжээний өөрчлөлт хийгдэх бүрд хэсэгчлэн, эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу холбогдох арга хэмжээг авч хэрэгжүүлэх;
19.2.6.мэдээллийн аюулгүй байдлын аудитыг хоёр жил тутамд хийлгэх;
19.2.7.мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлыг хангахад шаардлагатай удирдлага, зохион байгуулалтын болон техникийн арга хэмжээг төлөвлөх, хэрэгжүүлэх;
19.2.8.кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системтэй байх;
19.2.9.мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах;
19.2.10.кибер аюулгүй байдлын эрсдэлийн үнэлгээний болон мэдээллийн аюулгүй байдлын аудитын тайланг хүлээн авснаас хойш нэг сарын дотор кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлэх;
19.2.11.эрх бүхий байгууллагаас хүргүүлсэн зөвлөмж, шаардлагыг биелүүлэх, илэрсэн алдаа, зөрчлийг арилгах арга хэмжээг авах;
19.2.12.гадаадын иргэн, гадаадын хуулийн этгээдээр кибер аюулгүй байдлын эрсдэлийн үнэлгээг хийлгэх тохиолдолд тагнуулын байгууллагаас санал авах;
19.2.13.хариуцсан мэдээллийн систем, дэд бүтцийн хэвийн, найдвартай, тасралтгүй байдлыг хангах, гэмтэл саатлын үед сэргээн ажиллуулах төлөвлөгөөтэй байх;
19.2.14.кибер халдлага, зөрчлийн улмаас мэдээллийн систем, дэд бүтцийн хэвийн үйл ажиллагаа алдагдсан, тасралтгүй үйл ажиллагааг хангах боломжгүй болсон даруйд энэ талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд мэдэгдэх;
19.2.15.төлөвлөгөөт үзлэг шалгалт, өөрийн дэд бүтцээс гаднах сүлжээ, системд гарсан гэмтэл, саатал, гэнэтийн болон давагдашгүй хүчний шинжтэй нөхцөл байдлын улмаас дэд бүтцийн хэвийн, тасралтгүй үйл ажиллагааг хангах боломжгүй бол энэ талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төв, хэрэглэгчид даруй мэдэгдэх.

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

LAW ON CYBER SECURITY



AGAINST CYBER ATTACKS AND VIOLATIONS

NATIONAL CSIRT

134 GOVERNMENT ORGANIZATIONS WITH CRITICAL INFRASTRUCTURE

PUBLIC CSIRT

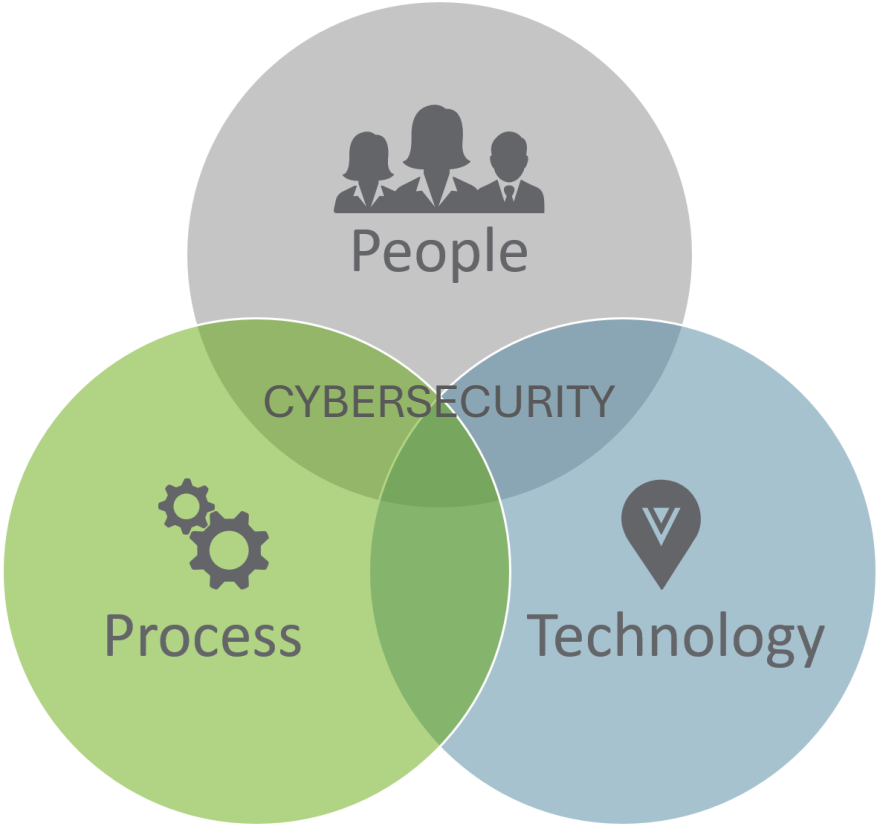
82 PRIVATE SECTOR LEGAL ENTITIES, INDIVIDUALS

ARMED FORCES CENTER

ARMED FORCES UNITS


CHALLENGES

CHALLENGES



КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

A Survey of 67 State Institutions

Parliament of Mongolia

5

Government agencies and organizations

28

Government of Mongolia

14

Office of the Provincial and Capital Governors

14

OTHER

5

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ТҮҮВЭР СУДАЛГАА

Ямар нэг байдлаар кибер халдлагад өртөж байсан	29.41%
Мэдээллийн технологийн асуудал хариуцсан нэгжгүй	32.35%
Мэдээллийн аюулгүй байдлыг хангах ямар нэгэн стандарт, фреймворк дагаж мөрддөггүй	53.33%
Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ хийлгэж байгаагүй	30.00%
Халдлагад өртөж байгаагүй, халдлагад өртөж байсан эсэхээ мэдэхгүй	70.59%
Мэдээллийн аюулгүй байдлын ямар нэгэн бодлогын баримт бичиггүй эсвэл боловсруулж байгаа	56.67%

2021 оны судалгаа

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

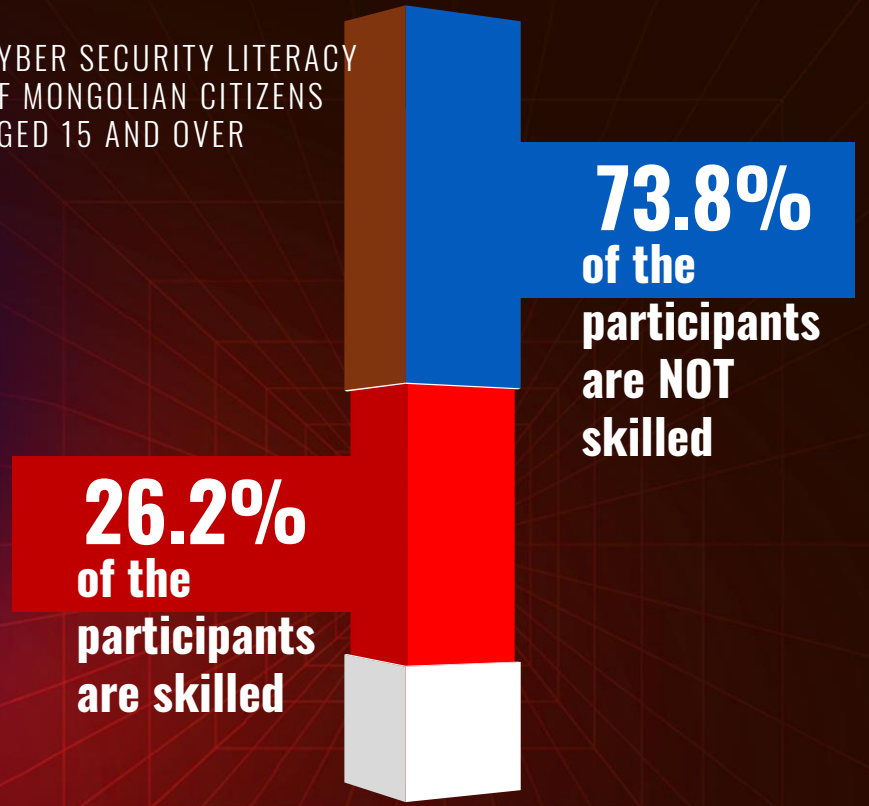
Improving Public Cybersecurity Knowledge

МОНГОЛ УЛСЫН ЗАСГИЙН ГАЗАР
ЦАХИМ ХӨГЖИЛ, ХАРИЛЦАА ХОЛБООНЫ ЯАМ

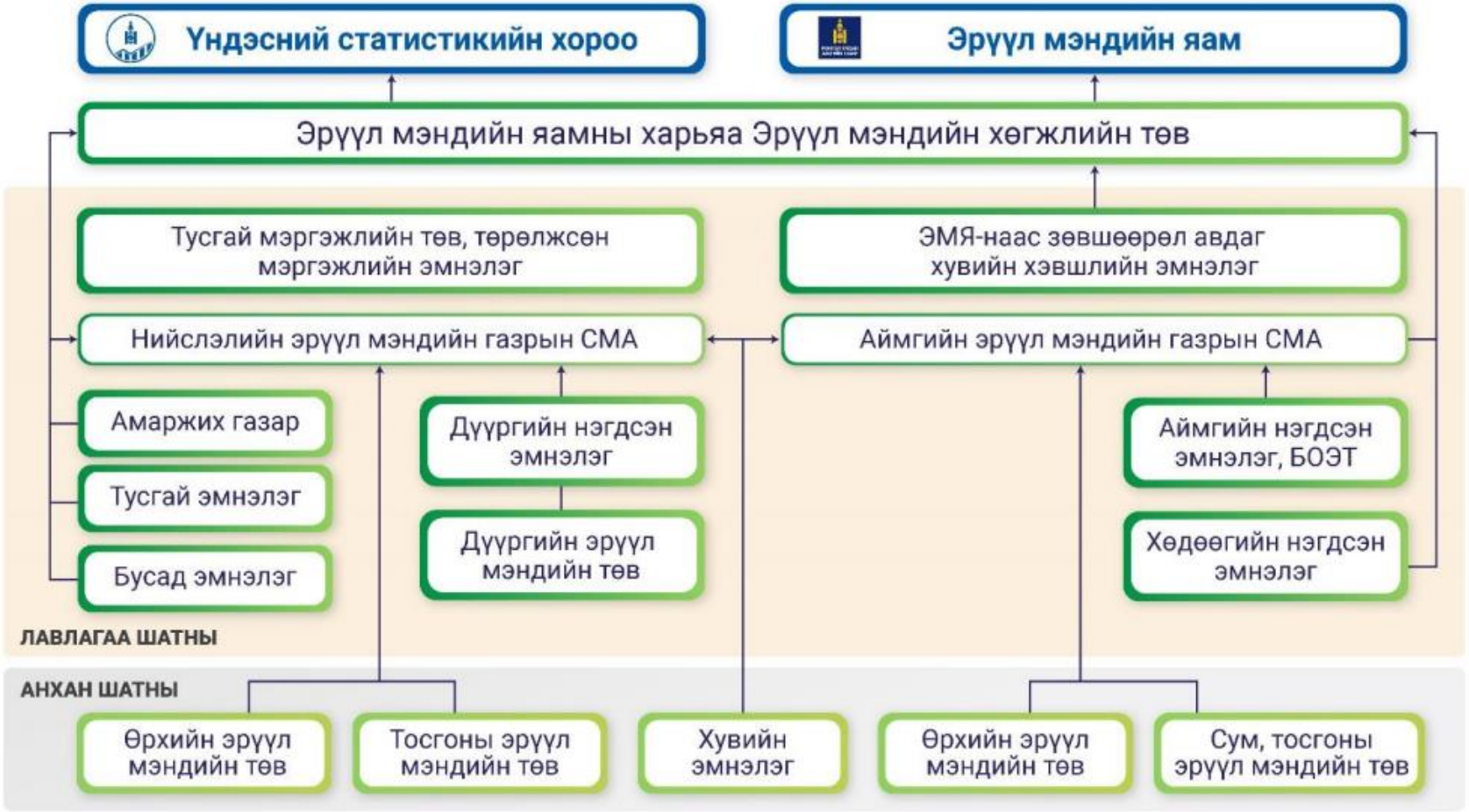
ҮНДЭСНИЙ СТАТИСТИКИЙН ХОРОО

2022 онд 6500 өрхийн 9144 иргэдийн дунд хийсэн судалгаагаар

CYBER SECURITY LITERACY OF MONGOLIAN CITIZENS AGED 15 AND OVER



Information sharing flow



КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

Software used in healthcare sector

21 VENDOR

37 SOFTWARE

- Лавлагаа шат: Люксембургийн Засгийн газрын санхүүжилттэй “Алсын зайн анагаах ухааны үндэсний сүлжээ” төсөл MNCARDIO
- Анхан шат: Зүрх судасны өвчний нэн шаардлагатай тусламж, үйлчилгээний багц МонПэн

- Монгол улсад чихрийн шижин, чихрийн шижингийн шалтгаант ретинопатийн тусламж үйлчилгээний загвар төсөл – ORBIS

- LICEMED
- Эмийн жор /ЭМД/

1. Эрүүл мэндийн статистик боловсруулалтын H-Info 3.0 програм хангамж
2. УОК дашбоард

1. Сурьеэгийн мэдээллийн систем TUUSBIS
2. Вирус хепатитын архаг халдвар бүртгэх систем
3. Томуугийн өвчлөл
4. EWAR

- Умайн хүзүү, хөхний өмөнгийн илрүүлэг үзлэгийн бүртгэл Screening.gov.mn

- Лабораторын мэдээллийн систем – LMIS BLOOD
- Хувийн лабоаторийн мэдээллийн системүүд

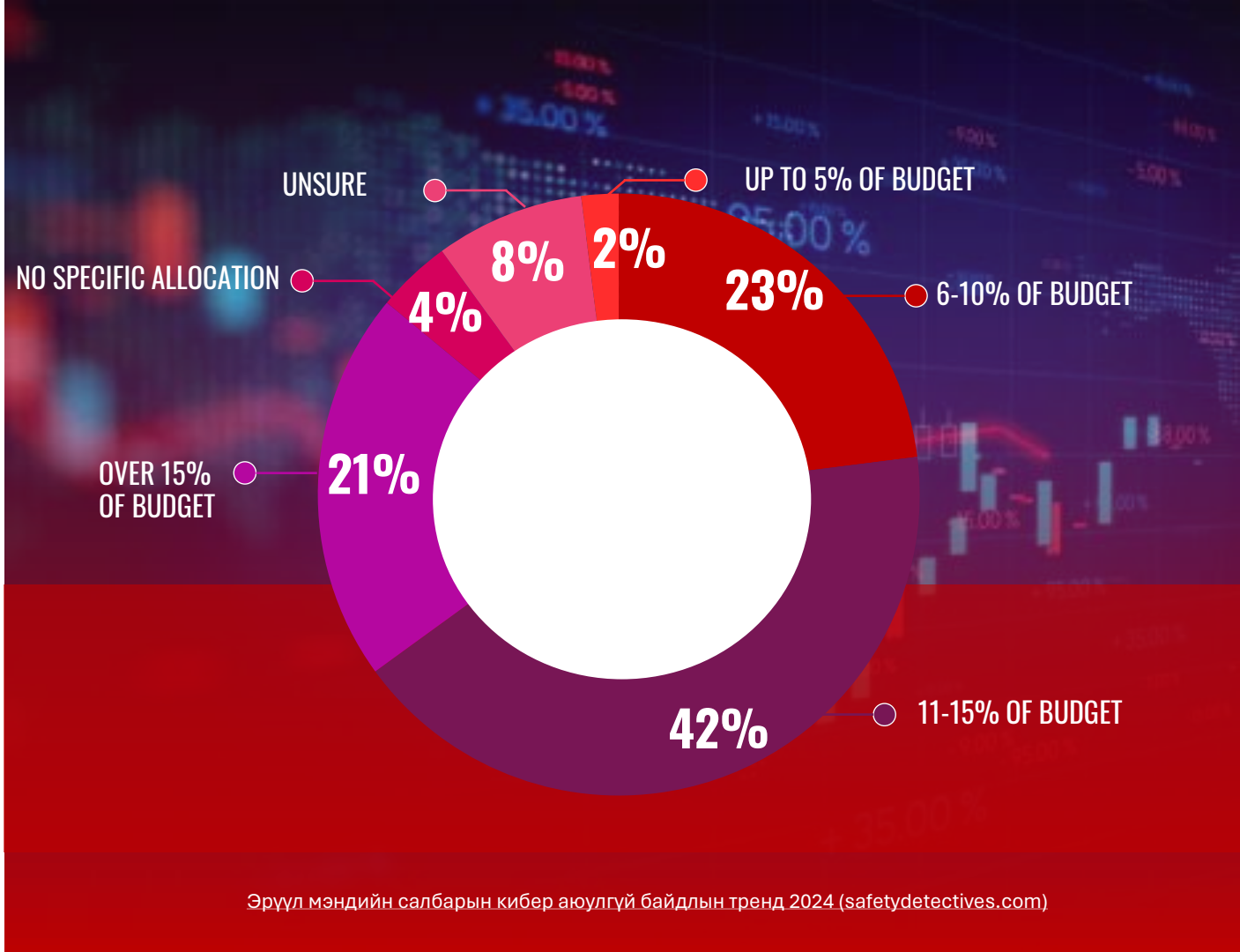
1. Өсвөр үеийн мэдээллийн систем
2. Эрт илрүүлгийн мэдээллийн систем VHS

1. Коронавируст халдвар /КОВИД/-ын цар тахлын үеийн мэдээ, мэдээллийн бэлэн байдлыг хангах, нэгдсэн сан үүсгэх зорилгоор
2. burtgel.mohs.mn,
3. eruul.gov.mn , ЭрүүлМН
4. tandalt.gov.mn

1. ЭМ-ИЙН ДААТГАЛЫН ЦАХИМ СИСТЕМ
- Элэг бүтэн монгол хөтөлбөр
- Дархлаажуулалтын систем

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ
НИЙТИЙН ТӨВ

HOW MUCH HEALTHCARE ORGANIZATIONS SPEND ON CYBERSECURITY WORLDWIDE, 2022



Эрүүл мэндийн салбарын кибер аюулгүй байдлын тренд 2024 (safetydetectives.com)

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

MAIN CHALLENGES

Information sharing

/Internal & external/

- Lack of knowledge
- Lack of human resource

Lack of cyber security knowledge of top management

Insufficient investment on cyber security

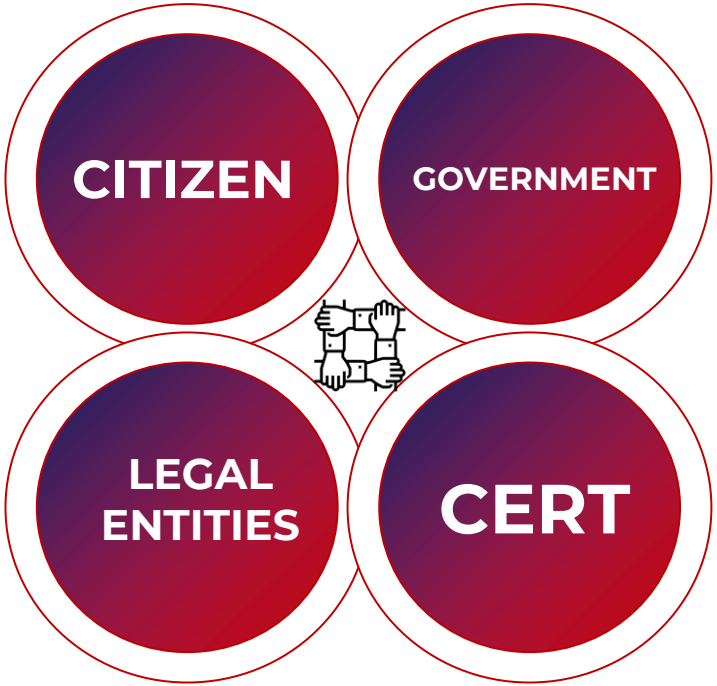
Implementing secure coding

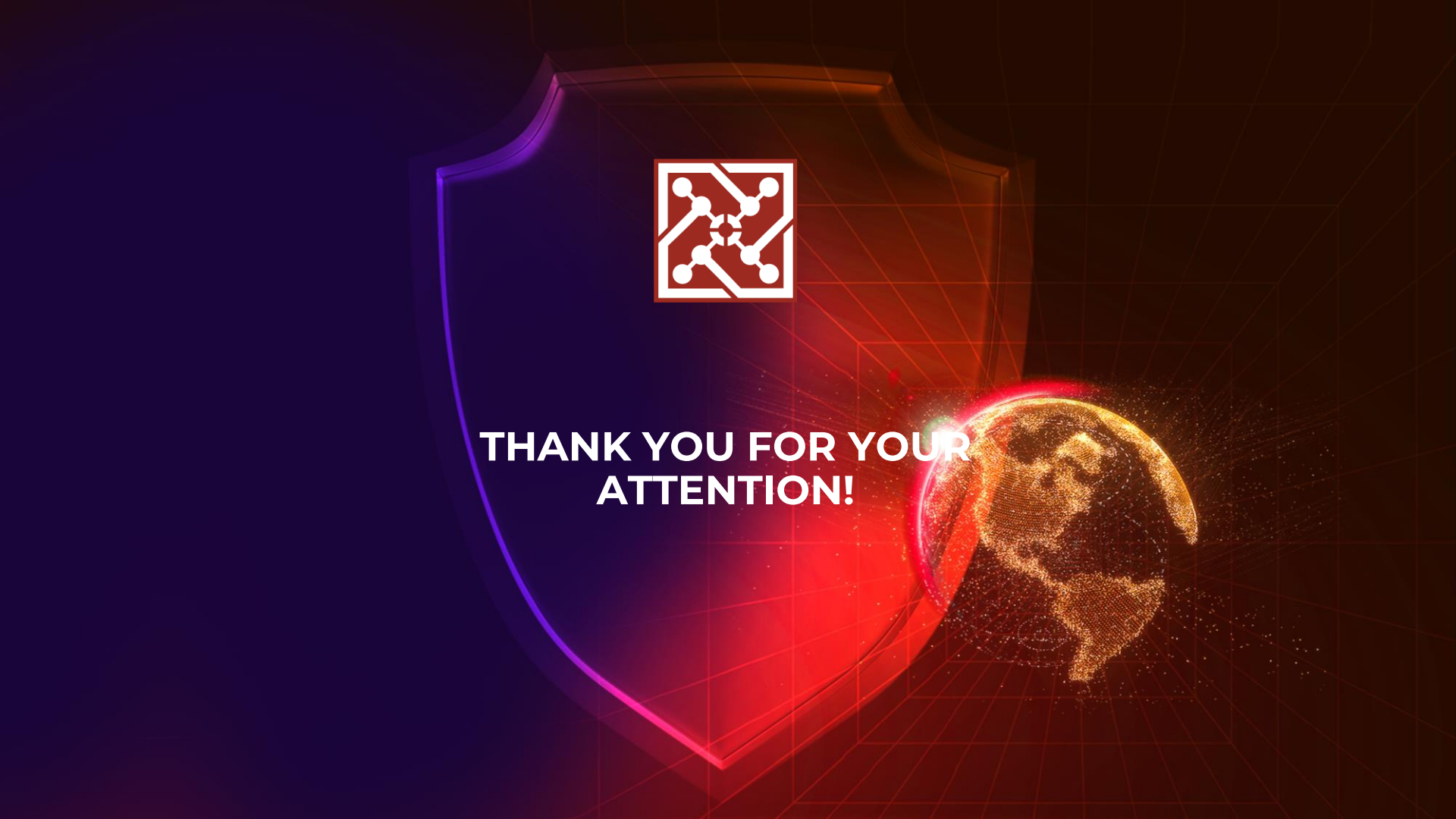
КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ
НИЙТИЙН ТӨВ

In maintaining cybersecurity,

everyone's participation is key

CYBER INDEPENDENCE OF MONGOLIA




THANK YOU FOR YOUR
ATTENTION!