RENOMIA

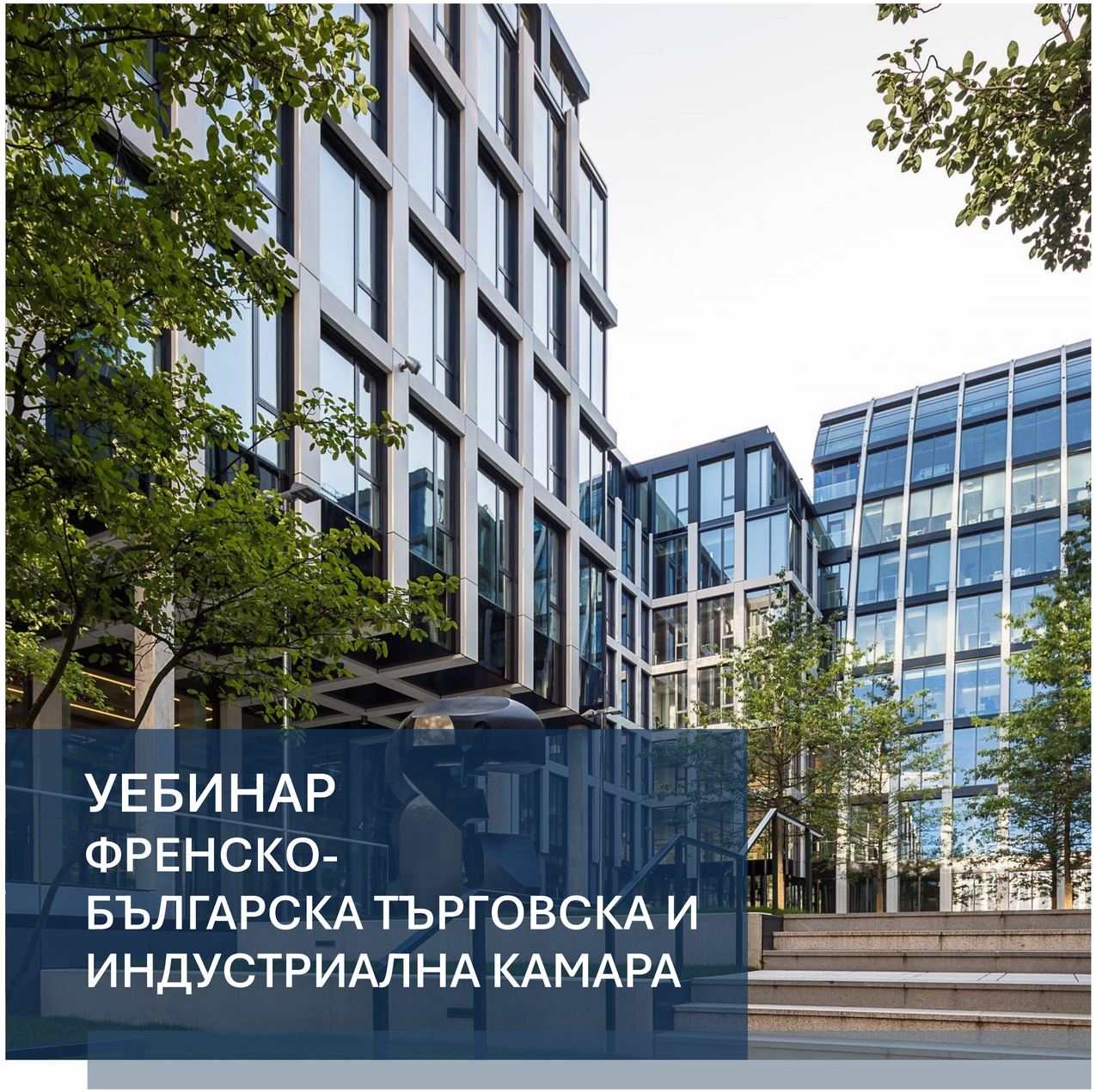
In partnership with

Gallagher

MIKOV & ATTORNEYS

CCI FRANCE BULGARIE
ФРЕНСКО-БЪЛГАРСКА
ТЪРГОВСКА
И ИНДУСТРИАЛНА КАМАРА

КИБЕРЗАСТРАХОВАНЕ В ЕРАТА НА ДИГИТАЛНИЯ РИСК



RENOMIA & Mikov Attorneys

25.06.2026

ДНЕВЕН РЕД

1. Кибер рискове, тенденции и състояние на пазара
2. Ключови аргументи в полза на киберзастраховането
3. Киберзастраховката на RENOMIA
4. Практически сценарии
5. Киберсигурност и правна рамка – GDPR, DORA и NIS2
6. Конкретни казуси от практиката
7. Процедури по възстановяването на вредите след кибератака

СРЕДА ОТ ДИНАМИЧНИ КИБЕР ЗАПЛАХИ

Data EUROPE 2025

80%

от докладваните кибератаки в Европа са насочени към малки и средни предприятия

+129%

ръст в киберинциденти с национално значение през 2025 г.

100 %

ежедневен ръст в появата на нови уязвимости, дори най-добрият ИТ екип не може да гарантира пълна защита

−11%

намаление в средните застрахователни премии

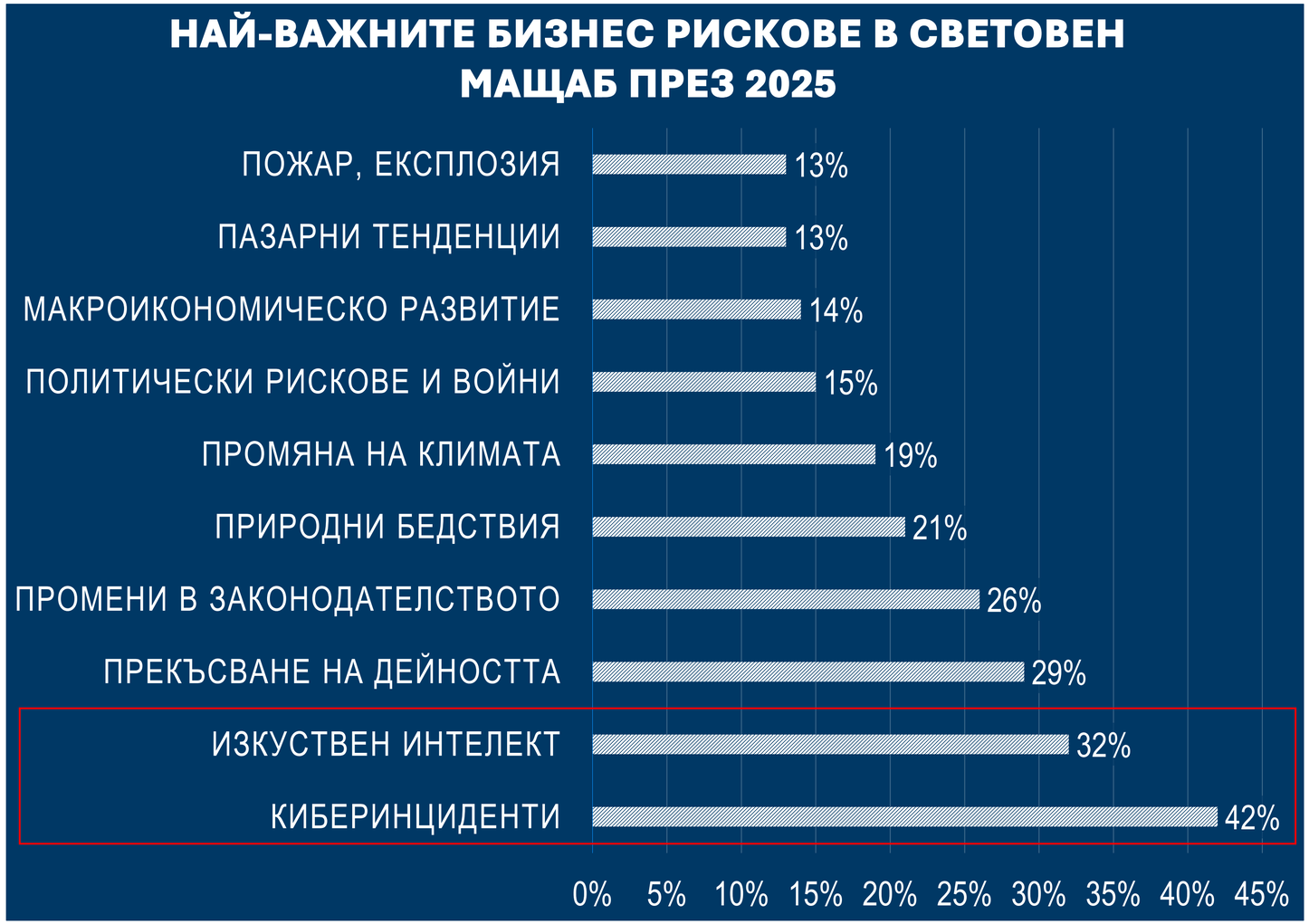
275%

увеличаване на атаките с рансъмуер, повишаващо риска от прекъсвания на дейността, което може да доведе до огромни загуби на приходи и екзистенциални заплахи

75%

от общия размер на изплатените суми по щети произтичат от едва 16% от уведомленията

КИБЕРИНЦИДЕНТИТЕ СА КЛАСИРАНИ № 1 ПО ВАЖНОСТ



№ 1 глобален риск

№ 1 за 5-та поредна година

Основен риск сред всички региони

Валиден за компании от всякакъв мащаб (вкл. МСП)

RENOMIA | In partnership with Gallagher | MIKOV & ATTORNEYS

Източник: Allianz Risk Barometer 2026

ОСНОВНИ ИЗТОЧНИЦИ НА ЗАПЛАХА

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ УСКОРЯВА РАЗВИТИЕТО НА КИБЕРЗАПЛАХИТЕ

- Рансъмуерът остава доминиращ вектор на атака
- Индустриализация на киберпрестъпността
- По-ниска бариера за навлизане за хакерите
- Силно насочени атаки с голям мащаб и пропорция

ЗАЩО КИБЕРЗАСТРАХОВАНЕТО Е ВАЖНО

Митове и факти

A. Моята компания не е цел	A. Повечето кибератаки не са с конкретна насоченост
B. Не съхраняваме чувствителни данни	B. Дори нечувствителни данни могат да представляват интерес за киберпрестъпниците
C. Разчитаме на нашия доставчик на ИТ услуги	C. Доставчиците на ИТ услуги не са специалисти по киберсигурност и не покриват финансови загуби
D. Предпочитаме да инвестираме в киберсигурност, вместо в киберзастраховка	D. Трябва да инвестирате и в двете. Дори при оптимална киберсигурност и защита, инцидент винаги може да се случи. Все пак имате и пожарогасител, и застраховка за пожар.
E. Една кибератака няма да наруши нашата дейност.	E. Компаниите са силно зависими от ИТ системите. Загубата на достъп до данни и системи обикновено има сериозни последствия.

RENOMIA CYBER FACILITY – ЕКСКЛУЗИВЕН КАПАЦИТЕТ

RENOMIA Cyber Facility:

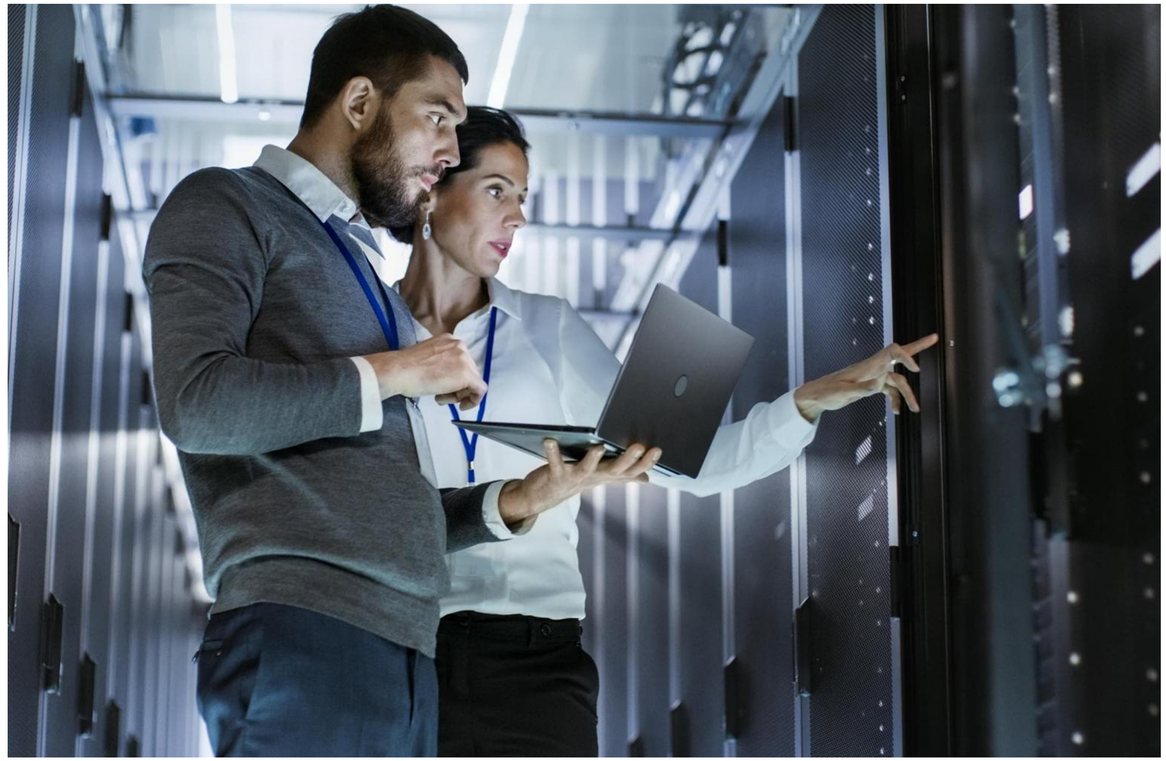
- **Покритие с лимит до €5 милиона**
- **Премии и самоучастия около 30–50% по-ниски** от стандартните оферти на пазара
- **Разширени покрития**, включително за киберпрестъпления с лимит €250,000
- **Бързо** получаване на оферта – до 5 дни
- **Лесно сключване** – без попълване на детайлен въпросник

RENOMIA | Gallagher Cyber Defence Centre

- **3 месеца безплатен** проактивен външен мониторинг на уязвимости

Какво не може да се застрахова чрез Cyber Facility:

- Клиенти с оборот над €500 милиона
- Клиенти в секторите:
  - Енергетика, Хазарт, Оръжейна индустрия, Космическа индустрия



ОБХВАТ НА ЗАСТРАХОВАТЕЛНОТО ПОКРИТИЕ

Разходи за реагиране на инциденти	Разходи за IT криминалисти, адвокати и кризисни консултанти, за реагиране на атаката и минимизиране на щетите.
Прекъсване на дейността	Загуба на печалба по време на прекъсване на работата на системите.
Възстановяване на данните и системите	Разходи за възстановяване на криптирани или изтрити данни, преинсталиране на системи.
Кибер изнудване	Разходи, свързани с преговори с хакери, евентуален откуп.
Уронване на репутацията	PR услуги, кризисна комуникация и маркетингови дейности за смекчаване на загубата на доверие след инцидент.
Отговорност за лични данни и мрежова сигурност	Разходи за уведомяване на субектите на данни, кол център, PR услуги.
Медийна отговорност	Разходи за съдебна защита и обезщетения в случай на съдебни искове за нарушаване на авторски права, клевета или неразрешено разпространение на онлайн съдържание.
Регулаторни глоби и санкции	Финансови санкции и съдебни разноски, произтичащи от нарушения на разпоредбите за защита на данните и поверителността – като например GDPR.
Спешно съдействие при инциденти	Незабавна 24/7 помощ (гореща линия, IT интервенция, кризисни мениджъри) в случай на сериозна атака.
Разходи за подобрения	Инвестиции за повишаване на сигурността след атака (напр. нова защитна стена, мониторинг), за да се предотврати повторение.
Киберпрестъпления, включително измами със социално инженерство	Покритие на финансови загуби, причинени от измама – например фишинг, измамни парични преводи или манипулиране на платежни нареждания.
Разходи за възнаграждения	Разходи за предлагане на възнаграждение за информация, водеща до залавянето или връщането на откраднати данни от извършителя.
Телекомуникационни измами	Възстановяване на разходи, произтичащи от злоупотреба с телефонни линии, VoIP системи или пренасочване на повиквания.
Cryptojacking	Разходи, причинени от неоторизирано използване на фирмената инфраструктура за добив на криптовалута.
Подмяна на хардуер (Bricking)	Възстановяване на разходи за ремонт или подмяна на физическо IT оборудване, ако то е унищожено или трайно повредено от кибератака.

ПРАКТИЧЕСКИ СЦЕНАРИИ

Човешка грешка

МЕНИДЖЪР „ЧОВЕШКИ РЕСУРСИ“ В КОМПАНИЯ ОТ СЕКТОРА НА ЗДРАВЕОПАЗВАНЕТО ПРИКАЧА ГРЕШЕН ФАЙЛ КЪМ ИМЕЙЛ, ИЗПРАТЕН ДО ЧЕТИРИМА КАНДИДАТИ ЗА РАБОТА. ФАЙЛЪТ СЪДЪРЖА ЛИЧНИ ДАННИ НА 43 000 БИВШИ СЛУЖИТЕЛИ.

		Размер на щетата:
Неправомерна обработка на лични данни	Разходи за съдебна защита във връзка с разследване от регулаторния орган	EUR 70,000
	Обезщетение за засегнатите служители	EUR 125,000
Разходи за реагиране на инцидента	Разходи за кризисен консултант	EUR 6,500
	Разходи за уведомяване на засегнатите	EUR 4,000
	Разходи за мониторинг за последващи вреди	EUR 16,000
	Разходи за правни консултации	EUR 12,000
Общо застрахователно обезщетение:		EUR 233,500

Кибератака (DoS)

ЦЕНТЪР ЗА ДАННИ, ХОСТВАЩ УЕБСАЙТА НА ВЕРИГА МАГАЗИНИ, СТАВА ОБЕКТ НА DoS КИБЕРАТАКА. В РЕЗУЛТАТ НА ТОВА УЕБСАЙТЪТ НА ЕЛЕКТРОННИЯ МАГАЗИН СТАВА НЕДОСТЪПЕН В ПРОДЪЛЖЕНИЕ НА НЯКОЛКО ЧАСА.

		Размер на щетата:
Разходи за възстановяване на дейността	Увеличени трудови разходи	EUR 11,000
	Разходи за външен доставчик на услугата	EUR 15,000
Прекъсване на дейността	Загуба на доход вследствие на свалянето на сайта	EUR 120,000
Разходи за реагиране на инцидента	Разходи за разследване на инцидента	EUR 15,000
	Разходи за правни консултации	EUR 12,000
	Разходи за кризисен консултант	EUR 8,000
Общо застрахователно обезщетение:		EUR 181,000

КИБЕРСИГУРНОСТ: ОТГОВОРНОСТ НА ПРЕДПРИЯТИЯТА

GDPR / NIS2 / DORA

МИС 2 - Директива за мрежова и информационна сигурност 2 (NIS 2), имплементирана от 2026 г. в Закона за киберсигурност (ЗК)

- Широк обхват: средно предприятие в определени сектори като енергетика, транспорт, банки и финансови инфраструктури, здравеопазване и др.
- Ръководният орган носи пряка отговорност за изпълнението на мерките за сигурност
- При неизпълнение: имуществена санкция в размер до 10 000 000 евро или до 2 на сто от общия световен годишен оборот (за важните субекти 7 000 000 евро или 1.4%), спиране на дейността (за съществените субекти) и др.
- По-лесно доказване на вредите към трети лица (тежестта за доказване на спазване на МИС 2 е за предприятието).

ОРЗД - Общият регламент относно защитата на данните (GDPR)

- Обработването на лични данни на физически лица (клиенти, служители, управители и др.), подходящи мерки за сигурност
- Санкция до 10 000 000 EUR или 2 % от общия му годишен световен оборот за предходната финансова година
- Отговорност за вреди към трети лица (82 ОРЗД)

Регламент за оперативна устойчивост на цифровите технологии (DORA)

- Кредитни институции, платежни институции, доставчици на услуги за предоставяне на информация за сметки, институции за електронни пари, инвестиционни посредници, доставчици на услуги за криптоактиви, централни депозитари на ценни книжа. Обхват и мерки за сигурност
- Лична отговорност за ръководни длъжности: от 5,000 до 10,000 евро.
- Санкция до 250,000 евро;
- По-лесно доказване на вредите към трети лица (тежестта за доказване на спазване на DORA е за финансовите предприятия)

КИБЕРСИГУРНОСТ – КОНКРЕТНИ КАЗУСИ ОТ ЮРИДИЧЕСКАТА ПРАКТИКА НА MIKOV & ATTORNEYS

Компютърна измама: смяна на банковата сметка на търговски партньор

Киберизмамниците получават достъп до кореспонденцията на дружество и неговия търговски партньор, като в даден момент променят банковата сметка на търговския партньор и плащанията се получават по банкови сметки в България.

Кибератака: Нерегламентиран достъп до информационната система на Инвестиционен посредник

Киберизмамниците получават достъп до корпоративни инвестиционни сметки на български ИП при трета финансова институция и нареждат финансови сделки от името на инвеститори - клиенти на ИП без тяхното съгласие/знание.

ПРОЦЕДУРИ ПО ВЪЗСТАНОВЯВАНЕТО НА ВРЕДИТЕ СЛЕД КИБЕРАТАКА

1. Граждански процедури в България

1.1. Обезпечение на иска (запор/възбрана), искове за възстановяване на вредите (неоснователно обогатяване, непозволено увреждане (деликт), договорна отговорност и др.)

1.2. Практически въпроси:

- Как да идентифицираме извършителя на кибератаката?
- Как да идентифицираме крайния получател на откраднатите средства?
- Кога жертвата носи отговорност за кибератаката пред своите клиенти и трети лица?

2. Наказателни процедури в България

2.1. Жалба, образуване на преписка, досъдебно производство, съдебно производство

2.2. Иск за вреди в съдебната фаза на наказателното производство от пострадалия (физическо или юридическо лице)

2.3. Проблеми от практиката: международен елемент на кибератаките - офшорни юрисдикции, трудно проследяване на финансовите транзакции извън ЕС, и др.

RENOMIA | In partnership with Gallagher

MIKOV & ATTORNEYS

ЗАСТРАХОВАТЕЛЕН БРОКЕР РЕНОМИА ООД

ПЛАМЕН ХРИСТОВ – Мениджър бизнес развитие

Тел.: +359 882 302 005

E-mail: plamen.hristov@renomia.bg

ИВАЙЛО ДИНКОВ – Мениджър клиенти

Тел.: +359 884 224 504

E-mail: ivaylo.dinkov@renomia.bg

АДВОКАТСКО ДРУЖЕСТВО МИКОВ И АДВОКАТИ

Адвокат КОНСТАНТИН МИКОВ

Тел.: +359 2 483 20 20

E-mail: info@mikov-attorneys.com

Благодарим Ви за вниманието!