KPMG

Кібердовіра 2022

Ключові висновки. Побудова довіри через кібербезпеку та конфіденційність

KPMG International

Зміст

Загальний огляд

П'ять найважливіших кроків у побудові довіри через кібербезпеку та конфіденційність

Для сучасного бізнесу довіра — це все. У непевному середовищі, яке постійно змінюється, клієнти, працівники та інвестори шукають організації, на які можна покластися. Проте створення та підтримка почуття довіри вимагає від організації взаємодії на всіх її рівнях для забезпечення узгодженого та єдиного бачення проблеми.

Сьогодні ми живемо у цифровому світі, і тому кожен аспект бізнесу залежить від чесності, цілісності та прозорості щодо збору та обробки інформації. Системи мають бути стійкими, надійними та здатними швидко реагувати на зміни, пов'язані з проривними технологіями. Кібердовіра має значення незалежно від того, чи є ви замовником послуг або клієнтом, який хоче відчувати себе в безпеці в процесі роботи з організацією, або частиною більш широкої екосистеми, що оточує кожну організацію і до якої належать партнери, інвестори, регулятори та супільство.

Кібербезпека та конфіденційність відіграють ключову роль у створенні та підтримці цієї довіри. Компанії нарощують темпи збору даних, розширюють використання технологій штучного інтелекту (ШІ), машинного навчання (МН) і впроваджують екологічні, соціальні та управлінські програми (ESG). У процесі цієї роботи компанії стикаються з дедалі жорсткішими нормативними вимогами.

Під час проведення нашого дослідження з питань кібердовіри KPMG Cyber trust insights 2022, ми опитали 1 881 керівника компаній і провели серію обговорень з керівниками та спеціалістами компаній з усього світу з метою вивчення того, наскільки вище керівництво компаній усвідомлює це, як воно долає виклики, що постають перед бізнесом, і що йому треба робити далі. Ми також дослідили ключову роль, яку можуть відігравати директори з інформаційної безпеки (CISO), допомагаючи керівникам компаній.

Ми визначаємо п'ять найважливіших кроків до побудови довіри через кібербезпеку: **сприймати кібербезпеку та конфіденційність як такі, що мають проходити червоною ниткою через весь процес ведення бізнесу; створювати внутрішні альянси; переосмислювати роль CISO; забезпечувати підтримку керівництва; а також підтримувати зв'язок з екосистемою.**

Передмова

Довіра в цифровому світі – цінний капітал та потужний рушій інвестицій

Довіра в цифровому середовищі – це впевненість зацікавлених сторін у тому, що організації здатні використовувати цифрові технології для захисту своїх інтересів і відповідати суспільним очікуванням та цінностям. Керівники компаній очікують на підвищення прибутковості бізнесу, краще утримання клієнтів та міцніші комерційні відносини від інвестицій в побудову більшого рівня довіри на підприємстві, що керується даними. Більшість організацій протягом наступних років планують впровадження нових цифрових інструментів – кожна нова цифрова ініціатива наражає на потенційні вразливості та репутаційні ризики.

Клієнти та суспільство очікують, що співпраця з організаціями, які щодня стикаються з викликами вразливості своїх ланцюжків поставок від кібератак, будуватиметься на надійності та професіоналізмі. І повномасштабна війна в Україні підкреслила це – вона винесла питання кібербезпеки та довіри у цифровому світі на новий рівень, підкреслила важливість формування кіберкультури на всіх рівнях організації, а до ролі директора з інформаційної кібербезпеки (CISO) додала нові сенси.

У новому глобальному звіті KPMG Cyber trust insights 2022 визначено п'ять важливих кроків до побудови довіри за допомогою кібербезпеки: формування відношення до кібербезпеки та конфіденційності як до невід`ємної частини бізнесу, створення внутрішніх альянсів; переосмислення ролі CISO, необхідність заручитися надійною підтримкою вищого керівництва, побудова відносин з кожним учасником екосистеми: партнерами, інвесторами, регуляторами та суспільством.

Олексій Янковський
Партнер, керівник практики з надання консультаційних послуг у сфері інформаційних технологій і кібербезпеки
KPMG в Україні

Ключові результати

Потік даних

Компанії масово збирають дані. Висловлюють занепокоєння щодо захисту, використання та обміну даними.

Більшість респондентів заявили про збільшення обсягів збору або аналізу даних щодо споживачів за минулий рік.

Інвестиції в напрями діяльності на основі даних стають все більш пріоритетними для організацій.

Виклики, пов'язані з штучним інтелектом та машинним навчанням

У суспільстві та бізнесі зростає занепокоєння щодо етики, безпеки та конфіденційності у зв'язку із застосуванням ШІ та МН під час аналізу великих масивів даних.

78% згодні з тим, що ШІ та МН містять в собі унікальні виклики щодо кібербезпеки.

3/4 заявляють, що ШІ та МН піднімають фундаментальні етичні питання.

Матеріальна вигода та довіра

Довіра важить більше, ніж будь-коли — і не тільки в плані репутації. Збільшення довіри створює конкурентні переваги та покращує кінцеві результати.

Понад 1/3 організацій визнають, що збільшення довіри веде до зростання.

Але 65% заявляють, що вимоги до захисту інформації визначаються скоріше необхідністю дотримання законодавства, ніж стратегічними амбіціями.

Посилення регулювання

Увага регуляторів зростає, і багато компаній занепокоєні тим, що орієнтуватися у глобальному регуляторному ландшафті стає все складніше.

36% занепокоєні щодо дотримання існуючих/нових вимог стосовно кібербезпеки у разі аутсорсингу робіт надавачам послуг з кібербезпеки.

34% занепокоєні вимогами до розкриття корпоративної інформації, пов'язаної з кібербезпекою.

Спільноти довіри

Очікується, що зовнішнє партнерство також буде життєво важливим для успіху в гіперзв'язаних екосистемах, але на шляху співпраці стоять практичні бар'єри.

79% заявляють про життєву важливість конструктивного співробітництва з постачальниками та клієнтами, але тільки 42% повідомляють, що співпрацюють із ними.

60% компаній визнають, що через їхні ланцюжки постачання вони є вразливими для кібератак.

Еволюція ролі CISO

Чи усвідомлюють організації роль, яку може відіграти CISO, допомагаючи їм запровадити загальний підхід до цифрової довіри?

1/2 виконавчих директорів висловлюють сумніви, що рівень довіри між Радою директорів та CISO можна охарактеризувати як «високий».

1/3 каже, що CISO не сприймаються як ключовий управлінський персонал і мають недостатній вплив для того, щоб захистити організацію та її дані.

Ціль, варта довіри

Чи усвідомили компанії зв'язок між кібердовірою та порядком денним щодо екології, соціальних питань і корпоративного управління (ESG)?

Менш як 1/5 каже, що команда CISO є невіддільною частиною команди ESG.

50% заявляють, що команда CISO грає дуже обмежену роль або не грає жодної ролі в ESG.

Джерело: KPMG Cyber trust insights 2022

1

Цифрова еволюція

Бізнес-кейс з інвестування у довіру

Що означає довіра?

Чітке визначення довіри може допомогти компаніям почати її вимірювати та збільшувати, а також відкриє для них широкий спектр відчутних переваг.

Цифрова довіра – це впевненість зацікавлених сторін у здатності організації використовувати цифрові технології для захисту власних інтересів і підтримки суспільних очікувань і цінностей.

Хоча кожна організація, ймовірно, матиме різні пріоритети та може застосовувати різні формулювання для опису аспектів цифрової довіри, це поняття зазвичай охоплює наступне:

Безпека та надійність

Покликані гарантувати надійний захист технологій і даних організації під час роботи відповідно до плану.

Інклюзивне, етичне та відповідальне використання

Покликані забезпечити, щоб організація розробляла, створювала та використовувала свої технології та дані на користь людям, суспільству в цілому, середовищу, в якому працює, та іншим зацікавленим сторонам.

Підзвітність та нагляд

Покликані гарантувати, що організація чітко визначає обов'язки щодо забезпечення надійності, розподіляє їх та контролює їхнє виконання.

Чому це важливо: зростання довіри може збільшити прибутки та лояльність клієнтів

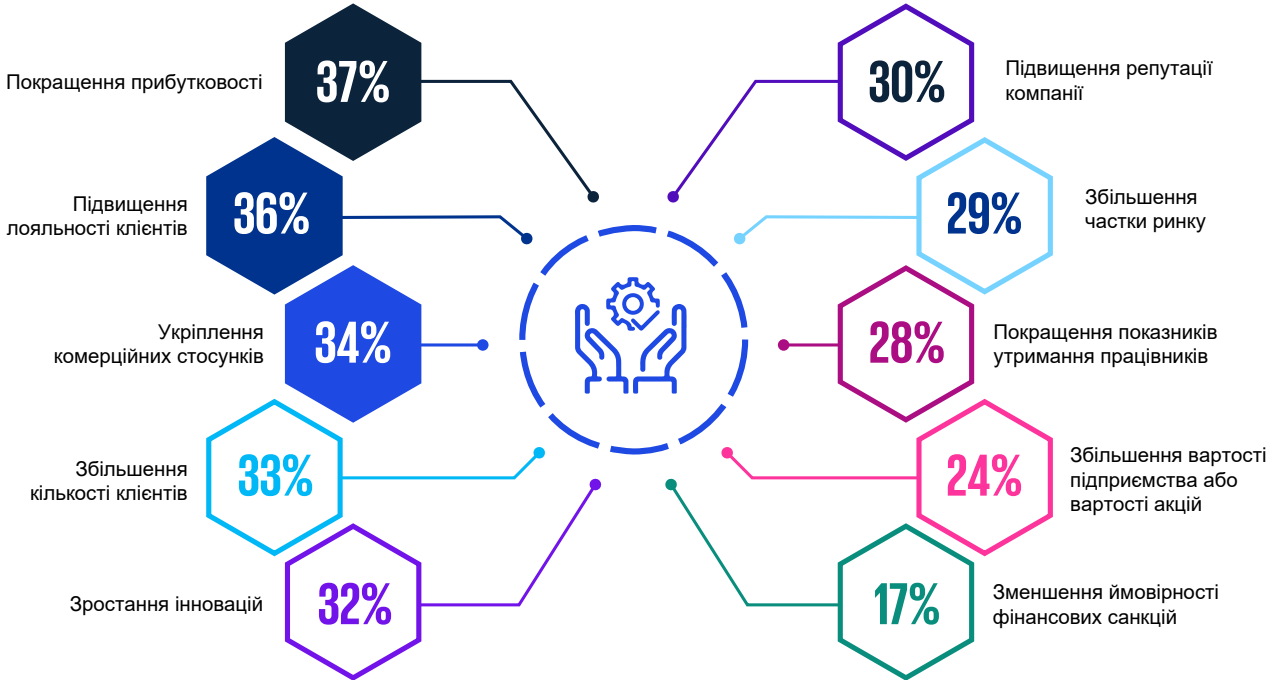
Наші респонденти виділяють три основні переваги, очікувані від зростання довіри:

1. Покращення прибутковості
2. Підвищення лояльності клієнтів
3. Укріплення комерційних стосунків

Інші потенційні здобутки включають зростання інновацій, покращення показників утримання працівників та збільшення частки ринку.

Головні переваги збільшення довіри

Нижче на діаграмі показаний % респондентів, які включили відповідний варіант до трьох основних.



Джерело: KPMG Cyber trust insights 2022

Бізнес інвестує в дані та зосереджує увагу на клієнтському досвіді

Цифрова трансформація йде повним ходом: у кожній галузі підприємства кардинально міняють свої технології та ставлять передові дані та складну аналітику в центр своєї діяльності. Протягом наступних 3 років організації планують здійснити низку інвестицій у цифрові інструменти, щоб стимулювати свій розвиток, оптимізувати взаємодію зі споживачами та клієнтами, оптимізувати бізнес-операції та отримати нові переваги від своїх даних. Кожна нова операція з даними несе в собі потенційні загрози та репутаційні ризики для компанії, від яких треба захищатися, щоб зберегти довіру.

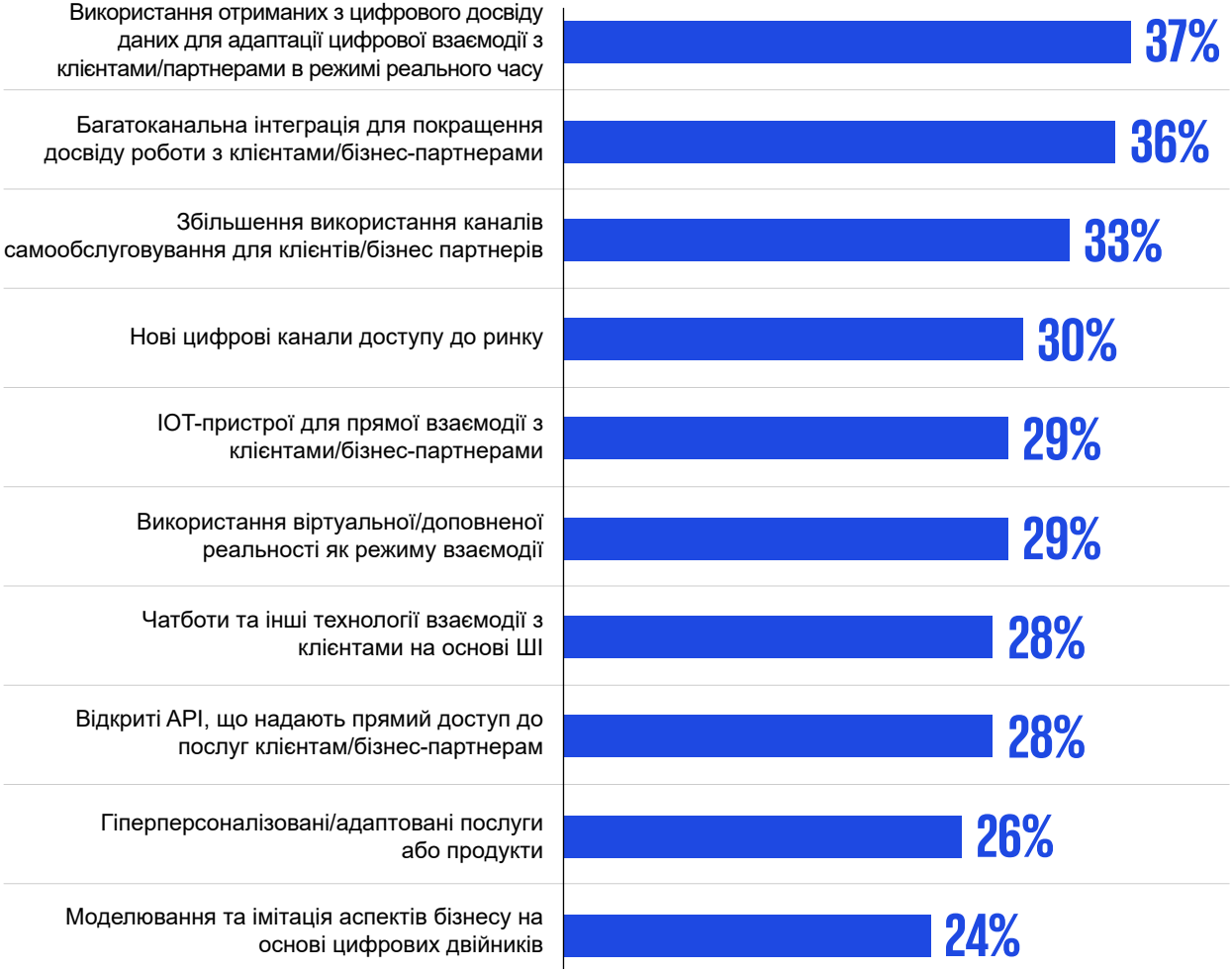
Згідно з KPMG's Global Tech Report, 61% компаній мають намір розгорнути нові платформи на основі проривних технологій упродовж 2 років, а також заявляють про те, що у наступні 3 роки вони нарощуватимуть інвестиції в інтернет речей (IoT), периферійні обчислення та технології 5G і, меншою мірою, технології віртуальної (VR) і доповненої (AR) реальності.

Також у даному звіті KPMG зазначено, що цифровізація каналів збуту розглядається організаціями як другий за своєю серйозністю виклик для кібербезпеки після створення гібридних робочих середовищ. Ми спитали компанії, в які цифрові аспекти вони інвестували. 37% компаній зосереджені на використанні отриманих з цифрового досвіду даних для адаптації цифрової взаємодії з клієнтами та партнерами в режимі реального часу, а 36% інвестують у багатоканальну інтеграцію з метою вдосконалення клієнтського досвіду.

У міру того, як ці тенденції набирають обертів у галузях, очікування клієнтів щодо конфіденційності також змінюються. Користувачі все частіше очікують, що вони матимуть можливість адаптувати контроль конфіденційності на своїх пристроях і каналах, вимагаючи від компаній включити гнучкі засоби контролю у майбутні продукти та послуги.

Основні сфери інвестування у цифровий досвід

Нижче на діаграмі показаний % респондентів, які включили відповідний варіант до трьох основних.



Джерело: KPMG Cyber trust insights 2022

> Інвестуючи в кібербезпеку та конфіденційність, ми керуємося прагненням захистити довіру з боку клієнтів"

Башар Абусеїдо
Старший віцепрезидент і CISO, Charles Schwab

Кібербезпека зазнає змін, а дані сьогодні важливі як ніколи

На цьому тлі компанії тепер повинні посилити заходи безпеки в тих сферах, які мають вирішальне значення для забезпечення довіри з боку зацікавлених сторін. Понад 80% наших респондентів визнали важливість покращення кібербезпеки та захисту даних, включаючи підвищення прозорості використання даних. Зокрема, 51% вважали захист IT-активів від атак надзвичайно важливим.

У міру того, як організації здійснюють цифрову трансформацію, необхідно буде закласти в бюджет інвестиції в кібербезпеку та конфіденційність, і це все більше розглядатиметься як невід'ємна частина цих стратегічних ініціатив. «Успіх трансформаційних цифрових послуг, швидше за все, залежатиме від того, чи зможуть організації інтегрувати безпеку та конфіденційність в їхню розробку та впровадження», – каже Аллан Кокріл, CISO корпорації Shell. – «Ми справді акцентуємо увагу на тому, що називаємо «безпекою через стандарти розробки», у тому, як створюємо технології. Ми хочемо, щоб ці стандарти були прозорими для наших клієнтів, оскільки наш обов'язок — підтримувати та зміцнювати довіру", - додає він.

«Інвестуючи в кібербезпеку та конфіденційність, ми керуємося прагненням захистити довіру з боку клієнтів», - зазначає Башар Абусеїдо, Старший віце-президент і CISO компанії Charles Schwab. – «Ми робимо все можливе, щоб зберегти довіру наших клієнтів за допомогою постійних удосконалень контролю конфіденційності та прозорості щодо того, яким чином ми захищаємо їхні дані».

Точка зору KPMG: довіра стає фундаментальним елементом нових технологій

Нові технології, такі, як технологія розподіленого реєстру (DLT), квантові обчислення, мережі 5G, ШІ/МН і технології доповненої та віртуальної реальності стрімко розвиваються й обіцяють змінити спосіб, у який компанії ведуть свій бізнес.

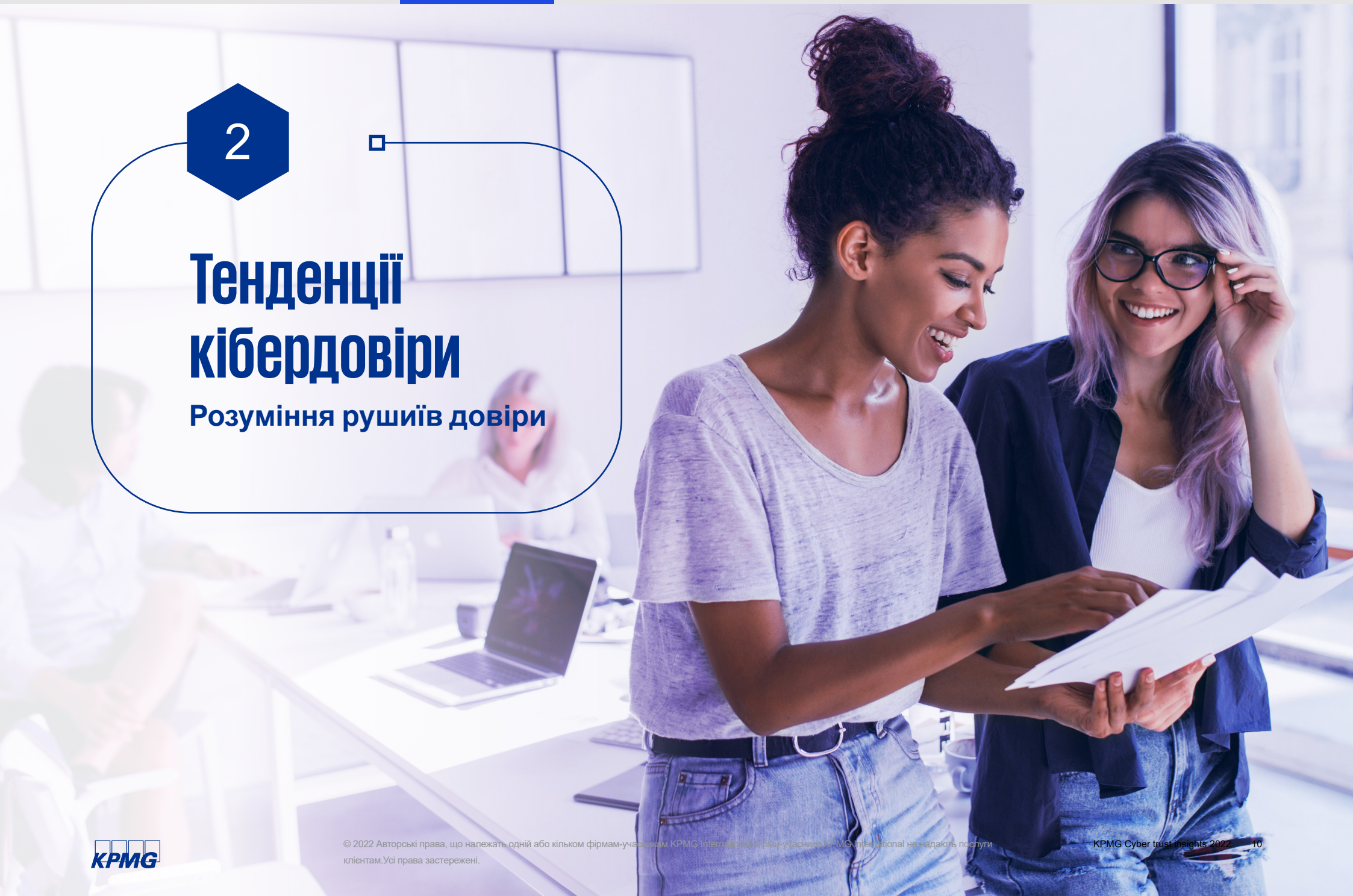
А втім, успішне розгортання майбутніх додатків (connected economy, смарт-контракти, NFT, метавсесвіт тощо), які спираються на ці технології, ймовірно, залежатиме від здатності організацій встановлювати довіру в багатьох вимірах. Це означає вбудову в роботу організації елементів керування безпекою та конфіденційністю, що забезпечують прозорість, надійність і цілісність.

Атул Гупта
Партнер, голова практики послуг із цифрової довіри та кібербезпеки
KPMG в Індії

2

Тенденції кібердовіри

Розуміння рушиїв довіри



Етичні виклики впровадження штучного інтелекту (ШІ)

Зростаюче використання технологій штучного інтелекту та машинного навчання в багатьох компаніях створює новий (і наразі погано зрозумілий) комплекс проблем довіри. Як показує дослідження KPMG, компанії налаштовані використовувати ШІ та МН з очікуваними перевагами для різних задач, від підвищення ефективності та продуктивності до прогнозного аналізу клієнтів і ринків.

Небезпека полягає в тому, що ці технології, якщо з ними поводитися неналежним чином, підвищують ризики кібербезпеки та конфіденційності, що може призвести до репутаційних втрат, і санкцій з боку регуляторних органів.

Організації починають усвідомлювати ці ризики. Понад три чверті наших респондентів (78%) погоджуються, що ШІ та МН створюють унікальні виклики щодо кібербезпеки.

Майже такий само відсоток вважає, що існують фундаментальні етичні питання, які треба вирішувати під час впровадження цих технологій, і заявляють, що організаціям потрібно буде більш відкрито ділитися інформацією щодо того, як вони це роблять.

Усі респонденти підкреслюють важливу роль, яку відіграють команди з кібербезпеки та конфіденційності, допомагаючи сформувати порядок денний щодо етики та управляючи ризиками.

«Ми багато працюємо над проблемою ворожого ШІ — таких викликів, як отруєння даних, предиктивна аналітика machine drift, атаки на ШІ — тому що вважаємо, що наступна хвиля атак відбудеться саме там», - вважає Енн Джонсон, віцепрезидентка Microsoft з розвитку безпеки бізнесу.

ШІ та МН створюють нові виклики для команд з інформаційної безпеки

Нижче на діаграмі показаний % респондентів, які погоджуються або повністю погоджуються з наведеними твердженнями.

78% Впровадження ШІ/МН створює унікальні виклики щодо кібербезпеки, які потребують особливої уваги

76% Впровадження ШІ/МН вимагає від нас додаткових заходів безпеки щодо того, як ми навчаємо системи ШІ/МН і контролюємо їхню продуктивність

76% Впровадження ШІ/МН вимагає від нас більш прозорої комунікації щодо використання нами методик ШІ/МН

76% Впровадження ШІ/МН піднімає фундаментальні питання етики, які потребують ретельного управління та нагляду

75% Впровадження ШІ/МН спричиняє ключові проблеми щодо дотримання нами конфіденційності під час збору й аналізу даних клієнтів та бізнес/партнерів

Джерело: KPMG Cyber trust insights 2022

Точка зору KPMG : етичний штучний інтелект

Організації знають, що вони повинні керуватися даними, бо інакше ризикують перестати відповідати вимогам дня. Багато з них масштабують ШІ для автоматизації прийняття рішень на основі даних, але ШІ несе нові ризики для бренду та прибутковості. Нові технології можуть сприяти нерівності та порушувати конфіденційність, а також обмежувати можливості автономного та індивідуального прийняття рішень.

Ви не можете просто звинувачувати саму систему штучного інтелекту в небажаних результатах. Надійний, етичний штучний інтелект – це не розкіш, а необхідність для бізнесу. Дедалі більше бізнес-лідерів усвідомлюють це, але довіру неможливо завоювати без докладання зусиль або подолання викликів.

Не в останню чергу те, що вважається етичним і заслуговує на довіру в одному секторі чи регіоні, може бути неприйнятним в іншому. Універсального рішення не існує, а копіювання того, що вже існує, є неефективним. Надійний штучний інтелект може бути досягнутий лише за допомогою цілісного, незалежного від технологій та широко схваленого підходу до обізнаності, управління ШІ та ризиками.

Наприклад, для оцінки впливу впровадження ШІ необхідно залучати відповідні зацікавлені сторони, що можуть виявити ризики. ШІ повинен узгоджуватися з моральними цінностями організації та зацікавлених сторін. Організації повинні ретельно оцінити відповідність законодавству та нормативним вимогам, а також прибуток на інвестиції від ШІ. Прийняті рішення мають відстежуватися та перевірятися. І всі вказані засоби захисту мають бути впроваджені без шкоди для інновацій.

Сандер Клоус
Партнер, Відділ розвитку бізнесу з даних та аналітики
KPMG в Нідерландах

> # Ми багато працюємо над захистом від ворожого ШІ, оскільки вважаємо, що наступна хвиля атак відбудеться саме там"
>
> **Енн Джонсон**
> віцепрезидентка Microsoft з розвитку безпеки бізнесу

Регуляторні перспективи

Зі зростанням стурбованості суспільства щодо довіри до цифрових технологій зростає також інтерес законодавців та регуляторів, які висувають все суворіші вимоги до прозорості та нагляду.

Джерело: KPMG Cyber trust insights 2022

36%

респондентів стурбовані своєю здатністю відповідати існуючим або новим нормам кібербезпеки в разі, коли діяльність передається на аутсорсинг.

34%

респондентів відчувають занепокоєння щодо розкриття інформації про кібербезпеку в корпоративній звітності.

31%

респондентів відчувають занепокоєння щодо зростаючих вимог стосовно об'єктів критичної інфраструктури, які є предметом посиленого регулювання у Великій Британії, ЄС та США.

На додаток до цього, міжнародні організації мають справлятися з дедалі складнішим, різноманітнішим та інколи суперечливішим розмаїттям екстериторіального регулювання. "Одна з проблем для CISO полягає в тому, що зацікавлені сторони в різних регіонах по-різному тлумачать одні й ті ж самі норми", - говорить Ульріх Байш, CISO компанії Bechtle, одного з найбільших європейських IT-провайдерів. - "Ви повинні мати чітке уявлення про те, що ви можете і чого не можете робити".

Точка зору KPMG: регуляторні чинники

В усьому світі прискорюється розвиток регулювання кібербезпеки та захисту персональних даних. Понад 137 країн зараз мають той чи інший режим захисту даних, часто претендуючи на екстериторіальну юрисдикцію над послугами, що пропонуються в певній країні, або над даними громадян такої країни. Більш зрілі режими захисту персональних даних переходять до другого покоління регулювання, стикаючись з новими викликами у сфері захисту персональних даних, зумовленими впровадженням технологій. Наприклад, дискусії щодо регулювання штучного інтелекту зараз формалізуються в законопроектах.

Крім того, країни впроваджують все більш суворі правила кібербезпеки критичної інфраструктури, оскільки зростає занепокоєння щодо атак на промислові системи управління. Ці правила переходять від вимог щодо проведення самооцінки до більш директивних рамок контролю, включаючи обов'язкове звітування про інциденти та зовнішній аудит.

Регуляторні органи також стають більш директивними у своїх системах контролю, одночасно прагнучи посилити незалежність CISO та їхню роль у встановленні стандартів внутрішнього контролю. У таких секторах як фінанси також з'являються більш комплексні вимоги до стійкості, націлені на відновленні бізнесу в екстремальних, але правдоподібних сценаріях.

Корпоративні вимоги до прозорості щодо кіберризиків обговорюються разом із зростанням вимог до розкриття інформації про інциденти, пов'язані з програмними вірусами-вимагачами. Компанії повинні інвестувати в автоматизацію процесу моніторингу та звітування щодо дотримання ними нормативних вимог, підтримувати регуляторний нагляд і враховувати тенденції у сфері регулювання конфіденційності та безпеки при розробці нових послуг та продуктів.

Девід Фербраш
Глобальний керівник напряму Майбутнє Кібербезпеки
KPMG International

Виходячи за рамки регулювання

Цифрова довіра повинна стати частиною порядку денного ESG, і, звичайно, кібербезпека та конфіденційність, ймовірно, стануть її частиною. "ESG є невіддільною частиною бізнесу в цілому, але, природно, Директор з інформаційної безпеки CISO відіграє ключову роль, зокрема, коли йдеться про соціальні та управлінські питання", - говорить Ульріх Байш з Bechtle.

Але для того, щоб це стало реальністю, необхідно докласти ще більше зусиль. Менш ніж одна з п'яти організацій описує функцію безпеки як невіддільну частину команди ESG, і при цьому більшість вважає, що вона відіграє дуже обмежену роль. Організаціям також необхідно визнати соціальні імперативи та зростаючі очікування щодо цих тем.

Особи, відповідальні за ESG, повинні співпрацювати в організаціях з тими, хто відповідає за кібербезпеку (найчастіше це - CISO) та конфіденційність даних (найчастіше це – спеціаліст із захисту даних (DPO)).

> **ESG є невід'ємною частиною бізнесу в цілому, але, природно, CISO відіграє ключову роль, зокрема, коли йдеться про соціальні та управлінські питання"**
>
> **Ульріх Байш**
> Директор з інформаційних технологій, Bechtel

Точка зору KPMG: ESG та соціальна відповідальність

Організації, які по-справжньому приймають порядок денний ESG, можуть заслужити довіру своїх клієнтів та зміцнити силу своїх брендів. У сучасному цифровому світі ради директорів, інвестори, регулятори, клієнти та широка громадськість очікують прозорої звітності в організації про стан кібербезпеки та конфіденційності.

Зацікавлені сторони хочуть бути впевненими в тому, що ради директорів і керівники розуміють соціальні наслідки прагнення забезпечити стійкість і цілісність критично важливих послуг, одночасно захищаючи інформацію, якій вони довіряють.

Ключові міркування для цих зацікавлених сторін включають таке:

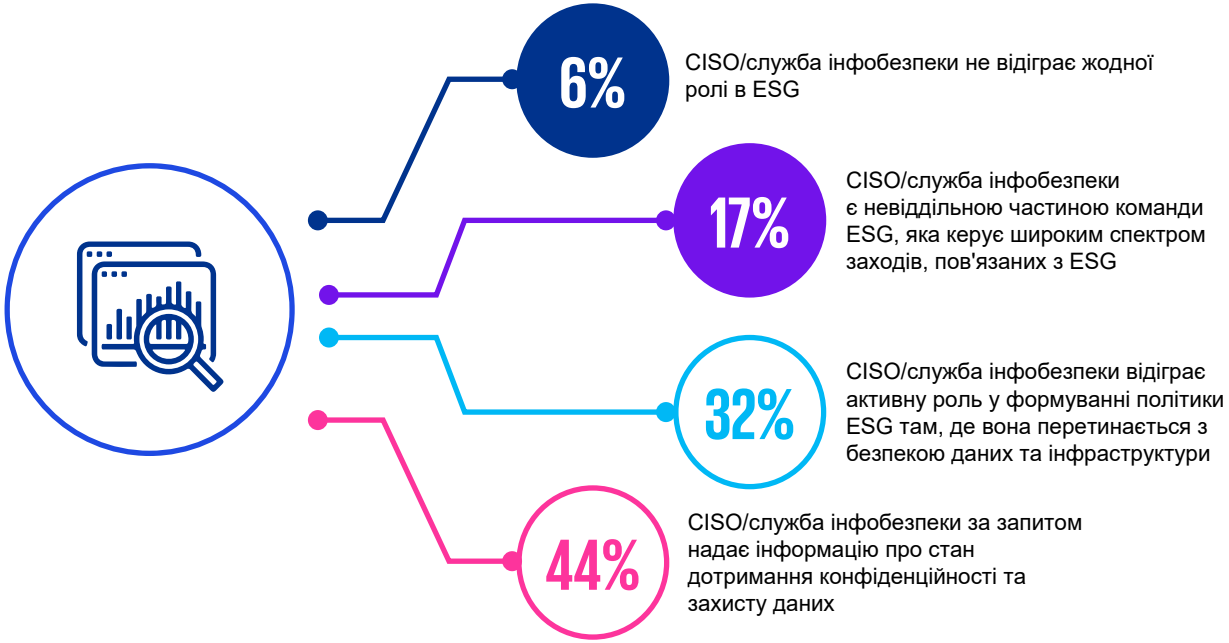
- Активний моніторинг цифрових активів з метою забезпечення доступу до безпечного та надійного контенту в умовах посилення використання та застосування інформації в режимі онлайн як зброї у вигляді "фейкових новин" та "глибинних фейків".
- Сприяння захисту клієнтів, особливо тих, хто перебуває за межею кібербідності, від шахрайства та крадіжки персональних даних за допомогою кібертехнологій.
- Прагнення забезпечити етичне впровадження таких технологій, як штучний інтелект і машинне навчання, які збирають та аналізують дані про клієнтів.
- Підтримувати надійність, цілісність і доступність цифрових послуг, на які ми, як суспільство, звикли покладатися.
- Демонстрація більш широкої прихильності до розбудови кібернавичок та потенціалу в рамках екосистеми своїх постачальників та за її межами.

Срінівас Потараджу
Партнер, практика цифрової довіри
KPMG в Індії

Сіддхарт Дурбха
Директор, практика цифрової довіри
KPMG в Індії

Більшість CISO лише пасивно залучені до політики та діяльності у сфері ESG

Нижче на діаграмі наведено відсоток респондентів, які обрали той чи інший варіант як найкращий.



Джерело: KPMG Cyber trust insights 2022

Точка зору KPMG: зміцнення довіри завдяки перевищенню мінімальних регуляторних вимог

Передові організації включають показники дотримання конфіденційності даних до системи звітності ESG.

Це дозволяє їм будувати довіру, одночасно допомагаючи забезпечити дотримання, як мінімум, регуляторних вимог. Часто в рамках зміцнення довіри організації активно намагаються перевищити мінімальні регуляторні стандарти, щоб зацікавлені сторони відчували себе більш впевненими в тому, що їх особиста інформація збирається, використовується або розкривається належним чином і не тільки з юридичної точки зору, але і з точки зору, яка вписується в наратив ESG сформульований організацією".

Сільвія Класовец Кінґзмілл
Керівник глобальної практики конфіденційності KPMG International та партнер KPMG у Канаді

3

Створення спільноти довіри

Сила співробітництва та партнерства

KPMG Cyber trust insights 2022 15

Сучасні компанії, які впроваджують цифровізацію, працюють не у вакуумі; вони все частіше стають активними учасниками більш широких партнерств та об'єднань. Це створює додаткові виклики командам з кібербезпеки: вони повинні зміцнювати довіру до екосистем, в яких діють їхні організації, співпрацюючи з партнерами для забезпечення взаємної довіри, а також довіри до екосистеми в цілому.

Сила в цифрах. В опитуванні KPMG Cyber trust insights 2022 майже половина наших респондентів (44%) стверджують, що співпраця з питань кібербезпеки в рамках більш широкої екосистеми допоможе їм, наприклад, передбачати атаки.

Хоча співпраця може бути бажаною, вона не завжди є простою. Понад третина респондентів (38%) стверджує, що на заваді зовнішньому партнерству в сфері кібербезпеки стоять питання конфіденційності, а 36% опитаних побоюються, що вони розкриють занадто багато інформації про свої власні заходи безпеки. Серед інших проблем - регуляторні обмеження, відсутність підтримки з боку вищого керівництва та брак ресурсів.

> **Але наявність стандарту і твердження, що правила вашого брандмауера відповідають цьому стандарту, - це зовсім інша інформація, що зазвичай не розкриває складних деталей і сприяє зміцненню довіри"**
>
> **Марк Томпсон**
> Директор зі стратегії, Міжнародна асоціація фахівців з питань конфіденційності (IAPP)

Співпраця з питань кібербезпеки в рамках ширшої екосистеми може допомогти організаціям краще передбачати атаки та відновлюватись після них

Нижче на діаграмі показаний % респондентів, які включили відповідний варіант до трьох основних.

Джерело: KPMG Cyber trust insights 2022

Практичні рішення існують, вважає Марк Томпсон, директор зі стратегії Міжнародної асоціації професіоналів з питань конфіденційності (IAPP). "Якби я надав вам параметри мого брандмауера, існує ризик, що ви побачите вразливість або прогалину", - говорить він. - "Але наявність стандарту і твердження, що правила вашого брандмауера відповідають цьому стандарту, - це зовсім інша інформація, що зазвичай не розкриває складних деталей і сприяє зміцненню довіри".

Несформованість стандартів та найкращих практик обміну інформацією може допомогти пояснити, чому менш як половина компаній співпрацюють або обмінюються інформацією з ключовими партнерами. Незважаючи на те, що 79% стверджують, що конструктивна взаємодія з постачальниками є життєво важливою для ефективної кібербезпеки, лише 42% респондентів кажуть, що вони дійсно працюють спільно для досягнення цієї мети.

Але це небажання може завдати серйозної шкоди. Понад половина компаній визнають, що не знають, чи їхній захист є достатньо потужним, щоб зупинити зловмисників від використання вразливостей у сфері закупівель та ланцюжків постачання.

Такий обмежений підхід до співпраці не може тривати далі; він не забезпечує достатнього захисту ані окремим організаціям, ані їхнім екосистемам, підриваючи довіру до обох. Понад половина наших респондентів (53%) занепокоєні тим, що їхні організації недостатньо активні у співпраці з питань кібербезпеки - і вони цілком можуть мати рацію.

Необхідно створення більшої кількості партнерств з кібербезпеки в усій екосистемі

Нижче на діаграмі показано відсоток респондентів, які обрали всі варіанти відповідей.

Джерело: KPMG Cyber trust insights 2022

Точка зору KPMG: цінність єдності

Ефективна розбудова спільноти є життєво важливою для вирішення проблем кібербезпеки: різні організації повинні працювати разом. Однак важливі питання щодо управління ризиками, репутації, права та стратегії все ще можуть перешкоджати досягненню цієї мети.

Жодна організація не може впоратися з цими викликами самотужки, тому важливо об'єднувати ресурси та ефективно координувати свої дії. Працюючи спільно, як державні, так і приватні організації можуть забезпечити додаткову ефективність, перспективи та ресурси.

Для розбудови довіри та спільноти кожна сторона має визнати, що є можливим, де існують бар'єри та як їх подолати. Наприклад, деякі організації використовують чинні протоколи, такі як настанови кібербезпеки NIST, для досягнення спільної мови та термінології у рамках партнерства з іншими організаціями. Інші зосереджуються на тому, як допомогти забезпечити збереження комерційної інформації в межах організації. Угоди про співпрацю, засновані на спільних принципах діяльності, можуть допомогти організаціям розвивати відносини і підтримувати цифрову інфраструктуру, зберігаючи при цьому конфіденційність та зміцнюючи взаємну довіру між партнерами.

Необхідно також визнати, що традиційна парадигма безпеки є менш актуальною в такому взаємопов'язаному ландшафті. Натомість більше сенсу має акцент на стійкому мисленні. Замість того, щоб намагатися перемогти зловмисників виключно шляхом ізоляції та за допомогою систем контролю, необхідний більш скоординований і колективний підхід.

Прасад Джаяраман
Керівник відділу з надання послуг з кібербезпеки
KPMG у США

4

Еволюція ролі CISO

Внесок CISO у побудову довіри

Введення позиції директора з інформаційної безпеки (CISO)

Іноді вважається, що CISO гальмують інновації та ініціативи щодо зростання, але зараз вони можуть відіграти вирішальну роль у створенні сприятливих для цього умов. Вони можуть стати рушійною силою успіху організації, діючи як один з головних охоронців довіри в організації.

"CISO дійсно можуть зміцнити та покращити довіру, але часто те, що вони роблять зазвичай визначається пріоритетами їхніх організацій", - каже Марк Томпсон з IAPP. "Існує потреба в тому, щоб вони почали входити в цей процес - допомагати організації рухатись і змінювати цю ситуацію".

Самі директори з інформаційної безпеки (CISO) усвідомлюють, що поставлено на карту. Понад три чверті респондентів (77%) кажуть, що посилення довіри є ключовою метою їхніх програм з управління кіберризиками.

При цьому організації демонструють високий рівень впевненості у своїх можливостях у сфері кібербезпеки: 74% стверджують, що за останні 12 місяців вони спостерігали покращення у сфері кібербезпеки, причому більш ніж кожна четверта з них зазначає, що це покращення було значним. Ця впевненість супроводжується твердою вірою в здатність CISO виконувати найважливіші задачі.

Але чи відчувають самі CISO, що вони здатні виправдати ці очікування?

Організації демонструють високий рівень довіри до CISO

Нижче на діаграмі показано відсоток респондентів, які оцінили кожен захід як "ефективний".

- **80%** Виконання законодавчих вимог до компанії у сфері кібербезпеки та захисту даних
- **80%** Впровадження технології, яка ефективно захищає дані клієнта/замовника/партнера
- **80%** Впровадження технологій, що захищають IT-активи від атак
- **79%** Проведення розслідувань та пом'якшення наслідків кібератак та витоків даних
- **79%** Підвищення прозорості стосовно використання даних та конфіденційності/захисту даних
- **78%** Підтримка освіти та підвищення обізнаності з питань кібербезпеки
- **78%** Налагодження співпраці з регуляторними органами, що створює відчуття взаємної довіри
- **78%** Робота із зацікавленими сторонами та інформування громадськості про наслідки кіберзлому
- **78%** Підтримка внутрішніх партнерів у трансформації бізнесу
- **77%** Укріплення кібербезпеки третіх сторін та ланцюгів поставок

Джерело: KPMG Cyber trust insights 2022

Цікаво, що багато директорів з інформаційної безпеки (CISO) намагаються отримати мандат для досягнення своїх цілей. За словами Енн Джонсон з Microsoft, часто доводиться мати складні розмови. "Якими даними ми будемо ділитися? Як ми будемо їх зберігати? Як ми збираємось використовувати їх з точки зору ШІ-МЛ? Як ми збираємося їх захищати? CISO повинен брати участь у кожній з цих розмов, і це нелегкі розмови", - додає Джонсон.

Майже дві третини респондентів (65%) стверджують, що інформаційна безпека розглядається в їхніх організаціях як діяльність, спрямована на зменшення ризиків, а не як чинник, що сприяє розвитку бізнесу. Більше того, 57% респондентів стверджують, що керівництво не розуміє конкурентних переваг посилення довіри внаслідок підвищення рівня інформаційної безпеки.

Чи свідчить цей факт про те, що CISO повинен робити більше для перевірки реальної ситуації з кібербезпекою?

Побудувати відносини з вищим керівництвом

Було б нереалістично і несправедливо очікувати, що CISO самостійно просуватимуть порядок денний щодо довіри в сфері кібербезпеки та конфіденційності даних. Їх взаємодія з колегами, такими як директор з питань захисту даних і директор з питань конфіденційності, ймовірно, буде мати вирішальне значення. Якщо вони будуть ефективно співпрацювати, це тріо може почати вносити практичні зміни для зміцнення довіри.

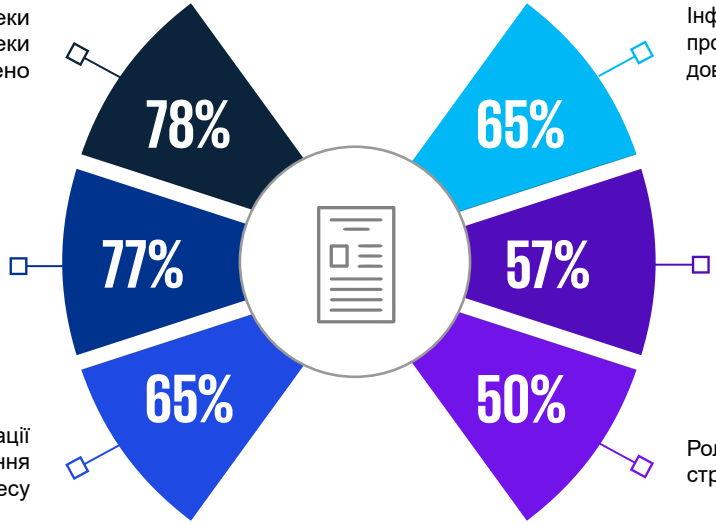
Хороша новина полягає в тому, що найвпливовіші лідери організацій вважають, що CISO і більш широка функція кібербезпеки повинні бути залучені до трансформації вже на ранній стадії.

45% респондентів з числа керівників вищої ланки вважають CISO ключовим виконавчим директором, а роль CISO за останні 5 років швидко підвищилася завдяки цифровій трансформації, підвищенню рівня кіберзлочинності та зростанню очікувань регуляторних органів.

Одним із способів для CISO змінити цю перспективу може бути зміщення фокусу з більш технічних питань - адже більше половини респондентів з числа керівників вищої ланки стверджують, що ради директорів все одно їх не розуміють. Перед CISO все ще стоїть завдання взяти на себе цю стратегічну роль. Компанії вимагають, щоб вони працювали на стратегічному рівні, зосереджувалися на потребах бізнесу і прагнули до того, щоб кіберпростір розглядався як червона нитка, що проходить через усі аспекти бізнес-стратегії, планування, інвестицій та реалізації.

Директори з інформаційної безпеки (CISO) готові діяти, але чи дозволять їм це зробити?

Нижче на діаграмі показано відсоток респондентів, які погоджуються або повністю погоджуються з цим твердженням.



Наша команда з інформаційної безпеки розуміє свою роль у забезпеченні безпеки нашої організації і відчуває себе впевнено

Інформаційна безпека в нашій компанії продиктована вимогами комплаєнсу, а не довгостроковими бізнес-амбіціями

Підвищення довіри з боку всіх зацікавлених сторін є одним з головних аспектів нашої програми управління кіберризиками

Наші вищі керівники недостатньо розуміють конкурентні переваги посилення довіри, що забезпечується кращою інформаційною безпекою

Інформаційна безпека в нашій організації розглядається як діяльність зі зниження ризиків, а не як засіб для ведення бізнесу

Роль нашого CISO не настільки стратегічна, як мала б бути

Джерело: KPMG Cyber trust insights 2022

Ради директорів компаній неоднозначно оцінюють вплив директора з інформаційної безпеки (CISO)

Нижче на діаграмі показаний відсоток респондентів, які вважають відповідні твердження вірними.

58% У відносинах між радою та CISO присутня значна довіра, вони консультуються між собою

54% Рада вважає, що CISO несе остаточну відповідальність за кібербезпеку організації

49% Рада розглядає інформаційну безпеку як вимушену необхідність, а не як спосіб отримання конкурентної переваги

36% CISO має менше впливу, ніж потрібно для захисту організації та її даних

31% Рада не вважає CISO ключовим керівником

31% Рада не розуміє технічних деталей, які надає йому CISO

Проблема кількісного визначення ризику

Багато організацій досягли значного прогресу в моделюванні та оцінці ризиків у цій сфері, відомій як така, що погано піддається аналізу. Три чверті організацій зазначають, що вони запровадили моделювання ризиків для кількісної оцінки та візуального звітування про кіберризики для правлінь своїх організацій, але лише 58% респондентів вважають «надійним» свій підхід до кількісної оцінки кіберризиків і погоджуються, що їхні сценарії кіберризиків адаптовані до потреб бізнесу.

Позитивним є те, що більше двох третин респондентів (69%) вважають, що вони використовують надійний підхід до оцінки кібердовіри, і не розглядають її як абстрактну концепцію. 65% опитаних стверджують, що моделювання ризиків стимулює інвестиції в поліпшення кібербезпеки, а також чіткий зв'язок між проектами та зменшенням ризиків.

Таким чином, CISO повинні робити більше, ніж вони роблять сьогодні. Їм необхідно усвідомлювати еволюційний характер своєї роботи, розширюючи сферу своєї діяльності там, де є потенціал для зміцнення довіри всередині організації та за її межами.

Точка зору KPMG: підтримка кількісної оцінки кіберризиків

Ретельне моделювання та кількісна оцінка можуть допомогти відповідальним за прийняття рішень особам зрозуміти справжній рівень кіберризику організації. Це може дозволити керівництву зрозуміти, які саме елементи управління найбільше сприяють зниженню певних кіберуразливостей, і допомогти зосередити свої ресурси на сферах з найбільшою віддачою.

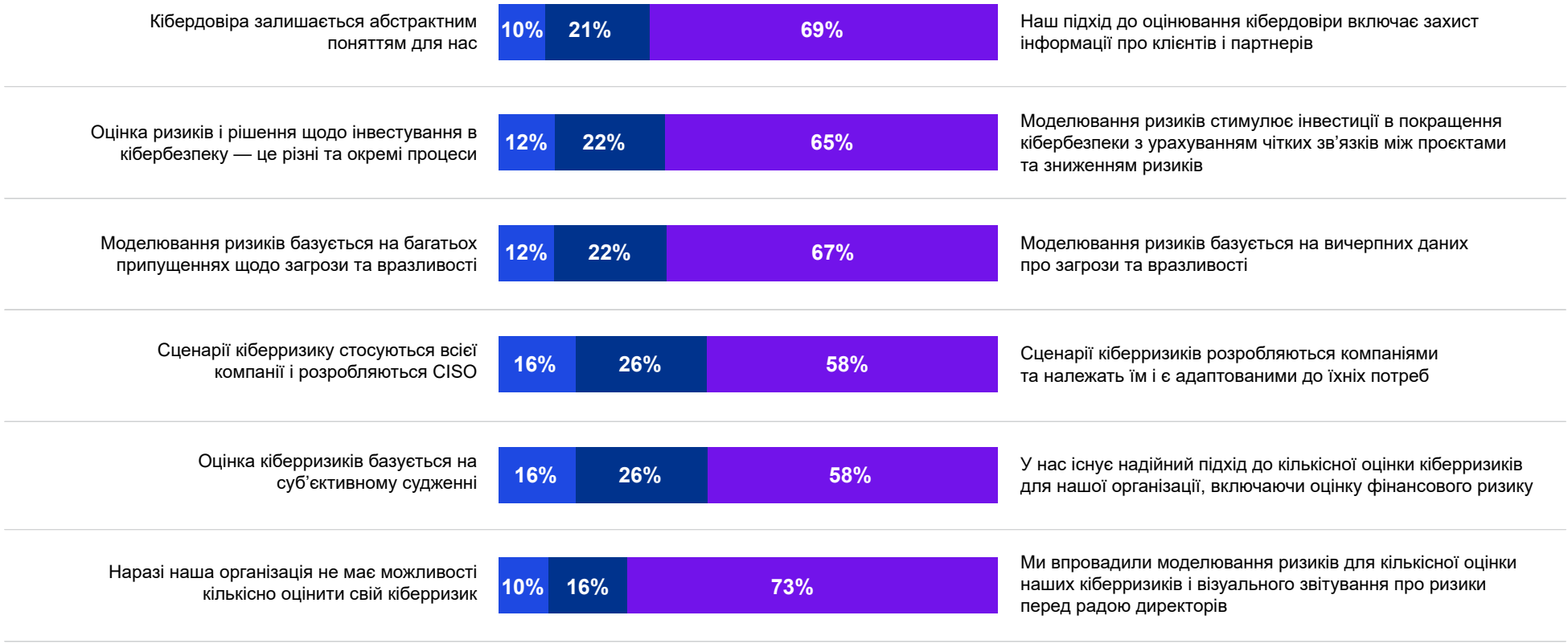
Для досягнення цього організації повинні дотримуватися п'яти принципів:

1. Забезпечення узгодження моделі ризику з організаційними рамками ризиків.
2. Послідовність у визначенні кіберризику як потенційних втрат для бізнесу (сценарії — чудовий спосіб це зробити).
3. Підхід до моделювання, що ґрунтується на загрозах, використовуючи моделювання шляхів атаки, щоб зрозуміти, як ці ризики можуть реалізовуватися.
4. Використання в розрахунках даних реального світу — оцінки ймовірності та впливу мають ґрунтуватися на внутрішніх і зовнішніх емпіричних даних (у вас їх є більше, ніж ви вважаєте).
5. Розуміння переваг та обмежень моделі та прозорість щодо них.

Джеймс Генбері
Директор служби кібербезпеки
KPMG у Великобританії

Багато організацій намагаються моделювати та оцінювати кіберризики

Нижче на діаграмі показано відсоток респондентів, які вказали, що відповідні твердження найточніше відображають їхню організацію.



Джерело: KPMG Cyber trust insights 2022

5

Місія здійсненна

Як організації можуть укріплювати довіру через роботу директора з інформаційної безпеки (CISO)

Керівники компаній розуміють, чому так важливо підвищувати довіру до своїх організацій та їх екосистем, і очікують, що директори з інформаційної безпеки (CISO) надаватиме їм підтримку в цьому питанні. Кібербезпека та конфіденційність є ключовими елементами в укріпленні довіри клієнтів, регулюючих органів та громадськості завдяки імперативу ESG.

CISO усвідомлюють свою відповідальність за просування компанії до цієї мети, як і їхні колеги в інших сферах бізнесу. Однак наше опитування показує, що багато хто насилу виконує цей обов'язок — можливо, тому, що їм не вистачає чіткого уявлення про те, що насправді означає кібердовіра і якою є їхня роль у завоюванні цієї довіри.

Цю роботу CISO не можуть виконувати поодинці. Їм потрібна більш суттєва підтримка з боку вищого керівництва, тісніша співпраця з іншими підрозділами організації та кооперація із зовнішніми партнерами та третіми особами.

А втім, роль CISO є життєво важливою. Чітке визначення довіри може стати гарною відправною точкою, що супроводжується використанням кібербезпеки та конфіденційності як способу зміцнення довіри до організації з усіма конкурентними перевагами.

Як організації повинні це зробити?

П'ять найважливіших кроків у побудові довіри через кібербезпеку та конфіденційність

01

Сприймати кібербезпеку та конфіденційність як такі, що мають проходити червоною ниткою через весь процес ведення бізнесу

Запроваджуйте кібербезпеку та конфіденційність у бізнес-процеси, управління та культуру організації, зробивши їх невіддільною частиною бізнесу, а не накладними витратами, пов'язаними з дотриманням нормативних вимог.

02

Створити внутрішні альянси для підвищення довіри

Співпрацюйте з такими колегами, як головний спеціаліст з питань обробки даних і керівник із питань конфіденційності, для встановлення, закріплення та підтримки кібердовіри.

03

Переосмислити роль CISO

Прийміть розширення порядку денного та визнайте здатність CISO зробити вагомий внесок у різних сферах, від ESG до етики ШІ.

04

Забезпечити підтримку інвестицій у довіру з боку керівництва

CISO, які заручилися підтримкою топменеджерів та ради директорів, швидше за все, буде легше просувати програму довіри. Це означає перетворення функціональних обов'язків CISO з вузько технічної ролі на стратегічну рушійну силу всередині організації.

05

Підтримувати зв'язок з екосистемою

Визначте ключових партнерів в екосистемі організації та тісно співпрацюйте з ними з метою підвищення довіри та стійкості.

Методологія та подяки

Про звіт KPMG Кібердовіра 2022

Дослідження KPMG Кібердовіра 2022 проводилося KPMG International у період з травня по червень 2022 року і включало опитування 1 881 керівника та проведення інтерв'ю з п’ятьма корпоративними лідерами з усього світу для вивчення ролі, яку відіграють кібербезпека та конфіденційність у розбудові та підтримці довіри.

Значна частка опитаних представлена вищим керівництвом компаній: 42% респондентів є членами ради директорів або керівниками компаній. Серед респондентів були лідери з 31 країни (24% з Азіатсько-Тихоокеанського регіону, 50% з Європи, Близького Сходу та Африки, 16% з Північної Америки та 10% з Південної Америки) та шести ключових галузей промисловості (енергетика та природні ресурси, фінансові послуги, галузь медично-біологічних наук та фармацевтика, ЗМІ, розваги та технології, державний сектор, телекомунікації).

Усі респонденти мають річний дохід понад 100 млн дол. США, 45% опитаних мають річний дохід понад 500 млн дол. США, 23% респондентів мають дохід понад 1 млрд дол. США та 7% керівників мають дохід понад 5 млрд дол. США.

KPMG висловлює подяку за внесок у проведення цього опитування:

- Башар Абусеїдо, старший віцепрезидент і CISO, Charles Schwab
- Ульріх Байш, IT-директор, Bechtle
- Аллан Кокріл, CISO, Shell
- Енн Джонсон, корпоративний віцепрезидент Microsoft Security Business Development
- Марк Томпсон, директор зі стратегії, Міжнародна асоціація фахівців із захисту конфіденційності (IAPP)

Про KPMG

Фірми KPMG можуть допомогти вам створити стійкий і надійний цифровий світ — навіть перед лицем нових загроз. Фахівці KPMG з питань кібербезпеки можуть запропонувати міждисциплінарний погляд на ризики, що дозволить вам забезпечити безпеку своєї організації, з надією дивитись у завтрашній день, швидше рухатися вперед та отримувати переваги завдяки використанню безпечних та надійних технологій.

Незалежно від того, де ви перебуваєте на шляху до кібербезпеки, фірми KPMG мають досвід на всіх рівнях організації — від організації роботи в залі засідань до центру обробки даних. Окрім оцінки вашої кібербезпеки та узгодження її з пріоритетами вашого бізнесу, ми можемо допомогти вам у розробці передових рішень, їх впровадженні, наданні порад щодо моніторингу поточних ризиків, а також допомогти вам ефективно реагувати на кіберінциденти.

Фахівці KPMG використовують технології, що постійно розвиваються, можуть об'єднувати та рухати бізнес вперед, зміцнюючи довіру, створюючи та захищаючи цінності, долаючи прірву між минулим і майбутнім.

Створимо надійний цифровий світ разом!

Контакти

Олексій Янковський
Партнер, керівник практики з надання консультаційних послуг у сфері інформаційних технологій і кібербезпеки KPMG в Україні

E: ayankovski@kpmg.ua

T: +380503157995

Геннадій Резніченко
Заступник директора практики з надання консультаційних послуг у сфері інформаційних технологій і кібербезпеки KPMG в Україні

E: greznichenko@kpmg.ua

T: +380504447525

Якщо Ви бажаєте отримати детальнішу інформацію про цей звіт або дізнатися, як KPMG може допомогти Вашому бізнесу, будь ласка, зверніться до: **markets@kpmg.ua**

Не допускається надання аудиторським клієнтам KPMG та їхнім афілійованим або пов'язаним особам деяких або всіх описаних в цьому документі послуг.

kpmg.com/socialmedia

Розроблено Evalueserve.

Назва публікації: KPMG cyber trust insights 2022 | Номер публікації: 138298-G | Дата публікації: грудень 2022