www.pwc.com/gsiss

Cybersecurity and Privacy

Посилення цифрового середовища проти кібер-загроз

Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки

pwc

Зміст

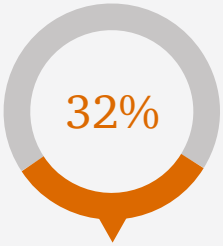
Пов’язані з кібербезпекою інциденти почали відбуватись частіше і регулярно потрапляють у заголовки новин, чим викликають все більшу тривогу у споживачів та керівників бізнесу. Незважаючи на пильну увагу до таких випадків, яка була привернута за останні роки, більшості організацій по всьому світу все ще важко осягнути і керувати виникаючими кіберризиками в усе більш складному цифровому середовищі. Зважаючи на те, що кожного дня цифрове середовище ускладнюється і наша залежність від даних та взаємодії у мережі зростає, розвиток стійкості до кіберзагроз – широкомасштабних подій з руйнівними наслідками, які розвиваються по каскадному принципу, ще ніколи не був настільки важливим.

Вже були зафіксовані поодинокі випадки кібератак, які мали вплив на життя та здоров'я людини, а також викликали ризики екологічних катастроф.[1] Разом з цими загрозами, деструктивний потенціал кібератак стає все більш очевидним, особливо у сфері геополітичних загроз. Наприклад, кібератака в Туреччині у грудні 2015 року вплинула на роботу мереж, які використовуються банками, засобами масової інформації та урядом країни.[2] Пізніше цього ж місяця вперше в результаті кібератаки на електроенергетичну систему були виведені з ладу системи розподілу електроенергії в Україні, залишивши без електроенергії 230 000 жителів.[3] Ця атака також була націлена на телефонну систему країни, що завадило користувачам повідомити про перебої у постачанні електроенергії і в результаті значно збільшило зусилля по відновленню енергопостачання.[4] У червні 2017 року кібератака вірусу шифрування Petya вразила українські комп'ютери та викликала операційні збої і простої як у цифровій, так і в операційній діяльності по всьому світу. На додачу до цього, ризики, пов'язані з масовим витоком даних, посилюють занепокоєність потенціалом впливу кібератак на глобальну економіку.[5]

Прогнозовані наслідки кібератаки на автоматизовані та/чи роботизовані системи

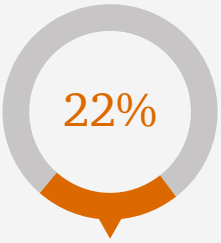
Порушення операційної/ виробничої діяльності

Втрата чи пошкодження конфіденційних даних



Негативний вплив на якість виробленої продукції

Пошкодження матеріального майна



Завдання шкоди людському життю

Джерело: Дослідження глобальних тенденцій інформаційної безпеки PwC 2018 року

1 The Cipher Brief, Cyber Deterrence Is Working – So Far, July 23, 2017
2 Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017
3 Wired, Inside the cunning, unprecedented hack on Ukraine's power grid, March 3, 2016
4 US Homeland Security Advisory Council, Final Report of the Cybersecurity Subcommittee: Part I - Incident Response, June 2016
5 The Wall Street Journal, The Morning Download, Sept. 11, 2017

Топ менеджери по всьому світу визнають зростаючу небезпеку кіберзагроз. У нашому дослідженні глобальних тенденцій інформаційної безпеки на 2018 рік керівники організацій, які використовують автоматизовані та роботизовані системи, відмічають усвідомлення значимості потенційних негативних наслідків кібератак. У якості основного можливого результату кібератаки 40% учасників опитування у світі називають порушення операційної діяльності, 39% - витік конфіденційних даних, 32% - завдання шкоди якості продукції, 29% - завдання фізичної шкоди майну та 22% - завдання шкоди людському життю.

«Багатьом компаніям потрібно провести переоцінку ризиків та сфокусуватись на підвищеній стійкості до неминучих загроз.»
– Шон Джойс, керівник практики в області кібербезпеки та конфіденційності PwC у США

Проте, не дивлячись на зростаючу обізнаність та публічний розголос подій та наслідків кібератак, багато компаній дотепер не підготовлені до реальної протидії загрозам. З 9500 топ менеджерів у 122 країнах світу, які були опитані в рамках нашого дослідження, 44% відповіли, що у них відсутня цілісна стратегія забезпечення кібербезпеки. Ще 48% повідомили, що не мають програми навчання співробітників та підвищення їх обізнаності у питаннях захисту інформації, а 54% заявили, що у них не передбачена політика реагування на надзвичайні ситуації. «Багатьом компаніям потрібно провести переоцінку ризиків та сфокусуватись на підвищеній стійкості до неминучих загроз» - сказав Шон Джойс, керівник практики в області кібербезпеки та конфіденційності PwC у США.

Широкий спектр коментарів про кіберзагрози, від відвертого перебільшення і створення міфу про кібер-армагедон до прямо протилежної позиції про буденний характер більшості кібератак, тільки створюють інформаційний безлад та вводять керівництво компаній в оману. Значно більш продуктивною стала б раціональна міжнародна дискусія, у результаті якої керівники компаній отримали б практичні рекомендації з підвищення стійкості своїх організацій до кібератак. В даному дослідженні та звіті ми ставимо перед собою саме таку мету.

Загальна кіберзалежність – ключовий фактор глобального ризику

Як було заявлено на Всесвітньому економічному форумі (ВЕФ), зростаюча взаємна кіберзалежність інфраструктурних мереж є одним з ключових факторів ризику у світовому масштабі. У доповіді Всесвітнього економічного форуму «Глобальні ризики, 2017 рік» йдеться про те, що кібератаки, дефекти програмного забезпечення та інші фактори можуть призвести до системних збоїв, які можуть «каскадно розповсюджуватись по мережам, впливаючи на суспільство найнеочікуванішим чином».[6]

Нещодавній звіт Ради національної розвідки США, присвячений глобльним тенденціям, також містить застереження про те, що суспільство стоїть перед «неминучим» ризиком кіберруйнування – потенційно у масовому масштабі та з «летальними наслідками» - за рахунок вразливості критично важливої інфраструктури.[7] Як показали ситуаційні дослідження катастроф некібернетичного характеру, події, які розвиваються по каскадному принципу, зазвичай починаються з порушення енергозабезпечення, що призводить до ураження ряду систем миттєво чи протягом доби. Таким чином, найчастіше на усунення початкової проблеми, до моменту її розповсюдження по каскадному принципу, є дуже мало часу.[8] Взаємозалежність між критичними чи не критичними IT-інфраструктурами зазвичай залишається непоміченою до виникнення аварійної ситуації.[9]

Більшість людей, особливо в Японії, США, Германії, Великобританії та Південній Кореї – занепокоєні можливістю здійснення кібератак з території інших країн.[10] Інструменти для здійснення кібератак стрімко розвиваються по всьому світу. Менші країни можуть мати можливості аналогічні можливостям великих держав. Витік хакерських інструментів Агентства національної безпеки США відкрив ці складні можливості для хакерів.[11] Говорячи про наслідки кібератак, більшість компаній, що стали їх жертвами, стверджують, що не в змозі визначити осіб, які вчинили злочин. В нашому дослідженні тільки 39% учасників глобального опитування заявили, що впевнені у тому, кого потрібно звинувачувати у кіберзлочині.

6 World Economic Forum, 2017 Global Risks Report, January 2017
7 US National Intelligence Council, Global Trends: Paradox of Progress, January 2017
8 CascEff, Cascading effects: What are they and how do they affect society? July 31, 2017
9 Internet outages after the Sept. 11, 2001, terrorist attacks were caused by a chain of events: lack of electric power required a major data center to use backup generators that relied on fuel; poor air quality in the city due to the attack hindered data-center cooling, hastening fuel consumption; normal fuel delivery was blocked by emergency traffic limits; and without fuel, the generators could not function. See Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017
10 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
11 PwC, Bold Steps to Manage Geopolitical Cyber Threats, 2017

39% учасників глобального опитування заявили, що впевнені у тому, кого потрібно звинувачувати у кіберзлочині.

Джерело: Дослідження глобальних тенденцій інформаційної безпеки PwC 2018 року

У дослідженні глобальних тенденцій інформаційної безпеки за 2018 рік ми виявили, що наявність у підприємств цілісної стратегії кібербезпеки особливо розповсюджена у Японії, де кібератаки розглядаються як одна з головних загроз національної безпеки.[16] Так, 72% респондентів із цієї країни відмітили, що мають таку стратегію. До числа лідерів по наявності цілісної стратегії кібербезпеки (74% респондентів) також можна віднести Малайзію, яка займає порівняно високе місце у Індексі кібербезпеки ООН. Обидві країни знаходяться у Азіатсько-Тихоокеанському регіоні, де за даними Всесвітнього економічного форуму, кібератаки входять до п'яти основних бізнес-ризиків.[17]

Високий рівень готовності не обов'язково означає низький рівень ризику. У глобальному індексі кібербезпеки 2017 року, який підготувала ООН, США входить у число країн-членів, які взяли на себе найбільший об'єм обов'язків у сфері кібербезпеки та поступаються по цьому показнику лише Сінгапуру. Однак, США поки що має вразливу інфраструктуру для тих факторів, які Всесвітній економічний форум вважає у якості бізнес-ризиків найбільш критичними на території північної Америки, а саме «масштабних кібератак чи впливу шкідливих програм, які викликають значні економічні збитки, геополітичну напруженість чи втрату довіри до мережі інтернет».[18] Міністерство внутрішньої безпеки США виявило більше 60 об'єктів критично важливої інфраструктури США, для яких збитки, викликані всього одним інцидентом у сфері кібербезпеки може закономірно призвести до економічних втрат у розмірі 50 млрд доларів США чи до 2500 випадків миттєвої смерті, або до серйозного зниження національної обороноздатності США.[19]

12 PwC, Uncovering the Potential of the Internet of Things, 2017
13 Then-US Director of National Intelligence James Clapper told Congress in 2016, "Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decision-making, reduce trust in systems, or cause adverse physical effects. Broader adoption of IoT devices and AI—in settings such as public utilities and health care—will only exacerbate these potential effects."
14 United Nations International Telecommunication Union, Global Cybersecurity Index report, 2017
15 The report ranked Singapore, the United States, Malaysia, Oman, Estonia, Mauritius, Australia, France, Georgia, and Canada as the most committed member states.

Для багатьох людей такі ризики є реальними. Дослідження, яке було проведено Pew Research Center, виявило, що абсолютна більшість американських громадян у найближчі 5 років прогнозують масштабні кібератаки на громадську інфраструктуру США чи на банківську та фінансову системи. Більшість спеціалістів в області інформаційної безпеки вважають, що критично важлива інфраструктура США піддасться кібератаці у найближчі два роки.[20]

Звідси виникає необхідність для усіх організацій – незалежно від того, на якій стадії готовності вони на їх думку знаходяться, - визначати і перевіряти успішність досягнення своїх стратегічних цілей у сфері кібербезпеки. Як зазначено у звіті Національної консультаційної ради Білого дому по інфраструктурі за серпень 2017 року, більшість системоутворюючих компаній у США не практикують базову кібергігієну, незважаючи на наявність та доступність відповідних ефективних інструментів та практик.[21] Насправді, як відмічають автори звіту, більшість компаній не обізнані у доступних федеральних інструментах для сканування, виявлення, усунення та захисту від кіберзагроз.

16 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
17 World Economic Forum, 2017 Global Risks Report shareable infographics, January 2017
18 World Economic Forum, 2017 Global Risks Report, January 2017
19 "Additional views" statement by Sen. Susan Collins (R-ME) in US Senate Report 114-32, April 15, 2015
20 Black Hat, The 2017 Black Hat Attendee Survey: Portrait of an Imminent Cyberthreat, July 2017

Стійкість – буфер для зниження ефекту від кібератак, якого потребує бізнес

«Завтра успішними країнами, - говориться у звіті Ради національної розвідки США від 2017 року – будуть, цілком ймовірно, ті країни, які інвестують в інфраструктуру, знання та взаємовідносини, і які будуть стійкі до потрясінь, - чи то економічні, екологічні, суспільні чи кібернетичні потрясіння». Аналогічна ідея може бути застосована і по відношенню до успішних компаній завтрашнього дня: найбільш стійкі з них будуть найкраще підготовлені для підтримки операційної діяльності, побудови відносин з замовниками, які базуються на довірі та досягнення високої економічної ефективності. Таким чином, підприємства можуть забезпечити стійкість, необхідну для амортизації підривної дії кібератак. Результати нашого дослідження пропонують відповіді на це запитання.

Керівники повинні брати на себе відповідальність за забезпечення стійкості до кіберзагроз. У приватному секторі особи, які керують своїм бізнесом, також повинні нести відповідальність за ризики, які супроводжують їх діяльність. Ради директорів повинні ефективно контролювати та превентивно керувати ризиками. Запорукою цього є стратегії підтримки неперервної господарчо-економічної діяльності, планування кадрової спадкоємності, стратегічної узгодженості та аналітичної обробки даних. Тим не менше, у рамках нашого дослідження було виявлено, що більшість корпоративних рад директорів не притримуються превентивного підходу до формування стратегій забезпечення кібербезпеки чи інвестиційних планів її розвитку.

Тільки 44% респондентів Дослідження глобальних тенденцій інформаційної безпеки PwC 2018 року заявили про те, що ради директорів активно беруть участь у розробці та реалізації загальної стратегії забезпечення безпеки їх компанії. «Більшість рад директорів як і раніше розглядають це як інформаційно-технологічну проблему» - каже Марк Олсен, співзасновник та президент з розвитку бізнесу та стратегії компанії IronNet Cybersecurity, у минулому керівник Національного контртерористичного центру США. За даними опитувань директорів державних та приватних компаній, проведених Національною асоціацією корпоративних директорів у 2016-2017 роках, лише деякі члени ради директорів мають тверду впевненість у тому, що їх компанії належним чином захищені від кібератак.[22] У подібних сумнівах, як правило, обумовлених слабкою залученістю рад директорів до питань безпеки, немає нічого дивного.

21 National Infrastructure Advisory Council, Securing Cyber Assets, August 2017

Трохи менше половини всіх глобальних учасників Дослідження глобальних тенденцій інформаційної безпеки PwC за 2018 рік вважають, що витрати на інформаційну безпеку мають бути засновані виключно на оцінці ризиків.

Більшість учасників нашого глобального опитування (66%) стверджують, що витрати їх організацій на забезпечення безпеки узгоджуються з прибутком по кожному з напрямків бізнесу. Однак значна частина (34%) вважає, що це не так, або вони не знають цього напевно. У такому контексті все більшого значення набуває посада директора з інформаційної безпеки. Згідно нашого дослідження, частіше директор з інформаційної безпеки чи директор з безпеки безпосередньо підзвітний головному директору чи раді директорів, аніж IT директору. «Директор з інформаційної безпеки повинен допомогти раді директорів визначити позицію компанії у відношенні захисту своєї корпоративної мережі – каже Кейт Александр, засновник та головний виконуючий директор компанії IronNet Cybersecurity, який раніше очолював Кіберкомандування США та Агентство національної безпеки у ранзі генерала. Інформація, яка надається, має включати в себе відомості про усі кібератаки, які відбувались, а також про недоліки у навчанні, обладнанні та інструментах у кіберсфері. Директор з інформаційної безпеки має акцентувати увагу на недоліках, щоб рада директорів могла виконувати свої обов'язки з урахуванням та повним розумінням ризиків, які стоять перед компанією».

Для виявлення прихованих ризиків бізнесу потрібно «копати глибше». Досягнення більш високого рівня кіберстійкості у рамках окремих підприємств чи всього суспільства вимагає більших зусиль із виявлення нових ризиків, які властиві сучасним технологіям, та керуванню ними. Організації мають потребу в правильному керівництві та процедурах впровадження заходів інформаційної безпеки, яких потребує цифровий прогрес. Проводячи цифрову трансформацію слід приділити особливу увагу захисту технологій та процесів, які впроваджуються, а у окремих випадках включити у цей процес трансформацію кібербезпеки. Сьогодні більшість компаній знаходяться лише на початку цього шляху.

22 Only 5% of public-company directors and 4% of private-company directors said they were "very confident." Most said they were only "moderately confident" (42% of public-company directors and 39% of private-company directors), according to survey data included in the National Association of Corporate Directors' 2017 Cyber-Risk Oversight Handbook

Кому підзвітний директор з інформаційної безпеки

Джерело: Дослідження глобальних тенденцій інформаційної безпеки PwC 2018 року

Наприклад, відносно невелика кількість наших респондентів заявила про те, що їх організації планують оцінити ризики, пов'язані з «Інтернетом речей», в рамках своєї бізнес-екосистеми. Сфера відповідальності за забезпечення безпеки «Інтернету речей» варіюється в залежності від організації: 29% респондентів стверджують, що це входить у обов'язки директора з інформаційної безпеки, тоді як інші вказують на інженерно-технічний персонал (20%) чи директора з управління ризиками (17%). Між тим, у багатьох організаціях до цього часу відсутні штатні позиції вищої ланки, в чию компетенцію входили б питання кібербезпеки. Тільки близько половини респондентів (52%), заявили про те, що в їх організації є посада директора з інформаційної безпеки; 45% респондентів сказали що у них є директор з безпеки, 47% повідомили що в їх компанії є спеціалізований персонал із забезпечення безпеки, в чиї задачі входить підтримка внутрішніх бізнес-процесів.

Стосовно управління ризиками, більшість організацій могли б діяти на випередження. Тільки половина респондентів говорить про те, що в їх організації проводяться спеціальні перевірки. Більшість ключових процесів виявлення кіберризиків у бізнес системах – включаючи тести на проникнення, оцінку загроз, активний моніторинг інформаційної

34%

респондентів заявляють, що їх організації планують проводити оцінку ризиків своєї бізнес-екосистеми, пов'язаних з «Інтернетом речей».

Джерело: Дослідження глобальних тенденцій інформаційної безпеки PwC 2018 року

безпеки, а також кіберрозвідку та оцінку вразливостей – впроваджені менше ніж у половини респондентів.

Необхідні більш активні зусилля з обміну інформацією та координацією дій між зацікавленими сторонами. Тільки 58% респондентів заявили про те, що офіційно співпрацюють з іншими представниками своєї галузі, включаючи конкурентів, у рамках підвищення рівня безпеки та зменшення ймовірності потенційного настання ризиків у майбутньому. **Достовірна, актуальна, корисна у практичному застосуванні інформація про кіберзагрози є ключовим фактором, який забезпечує можливість швидкого реагування та підтримки стійкості.** В різних організаціях, секторах економіки, країнах та регіонах створення потенціалу протистояння кіберзагрозам – це командна задача, ефективність вирішення якої буде тим менше, чим більше великих гравців залишаються в стороні.

Важливо обмінюватись інформацією, яка є корисною у практичному застосуванні. Серед учасників глобального дослідження PwC тільки половина впевнена, що їх зусилля призвели до обміну та отримання нової і корисної у практичному застосуванні інформації від їх колег по галузі.

Тільки половина респондентів говорить про те, що в їх організації проводяться спеціальні перевірки.

Джерело: Дослідження глобальних тенденцій інформаційної безпеки PwC 2018 року

Наступний крок за бізнес-лідерами

Перші особи компаній мають очолити зміни та залучити до них ради директорів. Топ менеджери компаній мають взяти на себе відповідальність за забезпечення кіберстійкості. Побудова вертикальної стратегії управління кіберризиками та ризиками конфіденційності вкрай необхідна в рамках усього підприємства. Концепція стійкості має бути інтегрована у комерційну діяльність. Стратегія компанії в області керування ризиками має базуватись на глибокому розумінні кіберзагроз, які стоять перед нею, та чіткому розумінні того, які ключові активи потребують найвищого рівня захисту. Необхідна цілісна концепція виявлення прийнятного рівня ризику. Керівництво має стимулювати розвиток культури управління кіберризиками на всіх рівнях організації.

Стійкість до кіберзагроз має розглядатись як невід'ємний компонент отримання вигоди, а не тільки як спосіб запобігання ризикам. Досягнення більш високого рівня стійкості до ризиків – це шлях до більш високої та довгострокової економічної ефективності. Так компанії, які інтегрували процедури керування неперервністю бізнес-процесів у свої програми управління ризиками підприємства до цунамі у Японії у 2011 році, змогли швидше конкурентів відновити операційну діяльність, що дозволило їм завоювати додаткову долю ринку у період після катастрофи.[23] Уряди країн всього світу переслідують довгострокові інтереси в області економічної та національної безпеки при розробці та розповсюдженні практик і технологій, які призначені для стимулювання розвитку стійкості ключових секторів економіки.

23 PwC, Building a Risk Resilient Organisation, 2012

Цільова співпраця та застосування досвіду на практиці. Галузеві лідери та державні діячі мають взаємодіяти, незважаючи на організаційні, секторні та національні кордони, щоб виявляти кіберризики та ризики міжмережевої взємодії, створювати карти ризиків та тестувати їх, підвищуючи стійкість підприємств та покращуючи управління ризиками. Необхідно спільно вирішувати проблеми, які пов'язані зі звітністю, обов'язками, відповідальністю, керуванням наслідками та нормами. Для цього компаніям слід капіталізувати наявну аналітичну інформацію:

- Необхідно робити висновки із ситуаційних досліджень, які присвячені реагуванню на катастрофічні події. Так, дослідження 2016 року, присвячене ключовим факторам, які дозволили достатньо ефективно відновити енергопостачання після потужного урагану «Сенді», виявило відсутність подібних факторів у сфері кібербезпеки. За підсумками даного дослідження були запропоновані способи побудови комплексних систем аварійного реагування, призначені для вирішення унікальних проблем, пов'язаних з кібератаками.[24]

- У випущеному Національною асоціацією корпоративних директорів «Довіднику з нагляду за кіберризиками за 2017 рік» підкреслюється, що членам рад директорів «необхідно забезпечити повну залученість керівництва у процес нарощення такої стійкості організаційних систем, яка була б економічно доцільною».[25] Принципи кіберстійкості, видані Всесвітнім економічним форумом для представників ради директорів у січні 2017 року, відносяться до числа доступних інструментів.

- Розробникам критичних систем слід проектувати їх таким чином, щоб відмови цих систем відбувались «якомога більш передбачувано і плавно», - відмічається у звіті американського Центру з визначення нових підходів до безпеки за 2014 рік.[26]

- Управлінські принципи, видані Організацією з інформаційного обміну та аналізу (ISAO), допоможуть зацікавленим суб'єктам економіки з більшою ефективністю ділитись інформацією та досвідом у сфері кіберзагроз.

- Звіт цільової робочої групи The New York Cyber Task Force від вересня 2017 року містить рекомендації з використання цілого ряду підходів із забезпечення кібербезпеки з метою досягнення максимального результату у потрібному масштабі при мінімальних витратах.

24 The Johns Hopkins University Applied Physics Laboratory LLC, Superstorm Sandy: Implications for Designing A Post-Cyber Attack Power Restoration System, March 2016
25 National Association of Corporate Directors' 2017 Cyber-Risk Oversight Handbook
26 Center for a New American Security, Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies, 2014

«Хмарні технології[27] мають величезний потенціал з покращення кібербезпеки шляхом створення архітектури та основи, яка була б безпечною у своєму початковому задумі», - відмічає Джейсон Хілі, виконавчий директор цільової робочої групи. «І ми ще не починали оцінку окупності» - каже Хілі.

- Нові дослідження можуть відкривати нові можливості. Так у вересні 2017 року Міністерство енергетики США анонсувало винагороду у розмірі вище 20 млн доларів для національних лабораторій відомства та їх партнерів за розробку інструментів забезпечення кібербезпеки, покликаних стимулювати стійкість та керування ризиками в рамках електромережевого господарства США, а також нафтогазової інфраструктури.[28]

Стрес-тест взаємозалежності. Для всіх ключових індустріальних секторів планети було б корисно провести стрес-тести їх взаємозв'язку з використанням модельованих сценаріїв кібератак, результати таких тестів мають бути вивчені та враховані особами, відповідальними за управління ризиками. Ден Гір, директор з інформаційної безпеки в компанії In-Q-Tel, відстоює необхідність розробки сценаріїв стрес-тестів кібербезпеки, покликаних відповісти на наступне запитання: «Чи зможу я витримати збій у роботі тих, від кого я залежу?».[29] У дослідженні за травень 2017 року, опублікованому Белферським центром науки та міжнародних відносин при Гарвардському університеті, відмічається така ж ідея, при цьому підкреслюється потенційна цінність регуляторів у секторах критичної інфраструктури чи незалежної перевірки результатів подібних тестів.[30]

Добровільні зусилля, які застосовуються зараз у фінансовому секторі, включають у себе ініціативу, висунуту Центром аналізу та обміну інформацією між фінансовими службами (FS-ISAC) з метою заснування Центру системного фінансового аналізу стійкості (FSARC) та Міжнародної федерації стійкості. Зусилля, подібні цим, можуть сприяти формуванню актуальних моделей забезпечення кібербезпеки в інших секторах економіки. «Центр FS-ISAC займається вивченням експериментально підтвердженого підходу до створення віртуального кіберполігону на якому підприємства могли б проводити модельовані ізольовані кібератаки для перевірки стійкості», - розповідає Білл Нельсон, президент і головний виконавчий директор цієї організації. У рамках енергетичного сектора раз в два роки проводяться навчання під назвою GridEx, мета яких полягає в імітаційному моделюванні кібер- та фізичних атак на електромережі та інші критично важливі об'єкти

27 For more discussion on the cloud, see PwC, Moving Forward with Cybersecurity and Privacy, 2017 and New York Cyber Task Force, Building a Defensible Cyberspace, Sept. 28, 2017
28 US Department of Energy, press release, September 2017
29 Dan Geer, For Good Measure: Stress Analysis, login: Volume 39, Number 6, USENIX, December 2014
30 Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017

інфраструктури на території Північної Америки. «Цим реалістичним військовим іграм немає аналогів», - відмічає Матт Олсен з компанії IronNet Cybersecurity.

Акцент на ризиках маніпулювання та знищення даних. У квітні 2017 року, Ден Гір в одному зі своїх виступів передбачив, що на зміну конфіденційності у якості найважливішої цілі забезпечення кібербезпеки у приватному секторі прийде цілісність. Він також додав, що у військовому секторі «види зброї, направлені на порушення цілісності, значно переважають аналогічні заходи проти конфіденційності».[31] Ініціатива створення «безпечної гавані» у фінансовому секторі могла послужити моделлю чи уроком для інших секторів при вирішенні проблем з появою непередбачуваних ризиків. «У рамках даних зусиль розробляються стандарти, покликані допомогти банкам повертати і відновлювати фінансову інформацію у випадку масштабної кібератаки», - відмічає Нельсон. Нова практична інструкція Національного інституту стандартів та технологій (NIST), «Цілісність даних: відновлення після атак вірусів-вимагачів та інших деструктивних подій», видана в попередній редакції у вересні 2017 року,[32] містить рекомендації з ефективного відновлення після подій, які призвели до порушення цілісності та (чи) доступності даних. Крім цього, використання технології блокчейн є тією сферою, для якої «особливо актуальне критичне значення цілісності транзакцій чи даних», як раніше відмічалось у проекті звіту Консультативного комітету по зв'язку у системі національної безпеки США.[33]

Основний підсумок полягає у тому, що у сучасних лідерів є можливість підвищити стійкість організацій до руйнуючих кіберзагроз та побудови безпечного цифрового середовища.

31 Dan Geer, closing keynote at SOURCE, Boston, April 27, 2017
32 US National Institute of Standards and Technology, Data Integrity: Recovering from Ransomware and Other Destructive Events, issued in draft in September 2017
33 US National Security Telecommunications Advisory Committee, Draft Report to the President on Emerging Technologies Strategic Vision, 2017

Методологія

Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік проводилось по всьому світу компанією PwC спільно з журналами CIO та CSO. Дослідження проводилось у мережі Інтернет у період з 24 квітня 2017 року по 26 травня 2017 року. Читачі журналів CIO та CSO та клієнти PwC з усього світу отримали запрошення на участь в опитуванні електронною поштою.

Результати, розглянуті у даному звіті, основані на відповідях більш ніж 9500 генеральних директорів, фінансових директорів, керівників управлінь з інформаційної безпеки, технічних директорів, віце-президентів та IT директорів з більше ніж 122 країн світу.

34% респондентів, опитаних у ході дослідження – з Північної Америки, 29% - з Європи, 18% - з Азіатсько-Тихоокеанського регіону, 14% - з Південної Америки та 1% з країн Близького Сходу та Африки.

Похибка становить менше 1%; через округлення сума усіх груп сукупно може не становити 100%.

Джерелом усіх чисел та графіків, які використовуються у даному звіті, є результати дослідження.

PwC cybersecurity and privacy contacts by country

Australia

Richard Bergman
Partner
richard.bergman@au.pwc.com

Steve Ingram
Partner
steve.ingram@au.pwc.com

Andrew Gordon
Partner
andrew.n.gordon@pwc.com

Megan Haas
Partner
megan.haas@pwc.com

Robert Martin
Partner
robert.w.martin@pwc.com

Austria

Christian Kurz
Senior Manager
christian.kurz@pwc.com

Belgium

Filip De Wolf
Partner
filip.de.wolf@be.pwc.com

Brazil

Edgar D'Andrea
Partner
edgar.dandrea@br.pwc.com

Canada

Sajith (Saj) Nair
Partner
s.nair@ca.pwc.com

David Craig
Partner
david.craig@pwc.com

Richard Wilson
Partner
richard.m.wilson@pwc.com

Justin Abel
Partner
justin.abel@pwc.com

Kartik Kannan
Partner
kartik.kannan@pwc.com

China

Ramesh Moosa
Partner
ramesh.moosa@cn.pwc.com

Kenneth Wong
Partner
kenneth.ks.wong@hk.pwc.com

Kok Tin Gan
Partner
kok.t.gan@hk.pwc.com

Marin Ivezic
Partner
marin.ivezic@hk.pwc.com

Chun Yin Cheung
Partner
chun.yin.cheung@cn.pwc.com

Lisa Li
Partner
lisa.ra.li@cn.pwc.com

Samuel Sinn
Partner
samuel.sinn@cn.pwc.com

Denmark

Christian Kjær
Partner
christian.x.kjaer@dk.pwc.com

Mads Nørgaard Madsen
Partner
mads.norgaard.madsen@dk.pwc.com

France

Philippe Trouchaud
Partner
philippe.trouchaud@fr.pwc.com

Germany

Derk Fischer
Partner
derk.fischer@pwc.com

India

Sivarama Krishnan
Partner
sivarama.krishnan@in.pwc.com

Indonesia

Subianto Subianto
Partner
subianto.subianto@id.pwc.com

Israel

Rafael Maman
Partner
rafael.maman@il.pwc.com

Italy

Fabio Merello
Partner
fabio.merello@it.pwc.com

Japan

Yuji Hoshizawa
Partner
yuji.hoshizawa@pwc.com

Sean King
Partner
sean.c.king@pwc.com

Naoki Yamamoto
Partner
naoki.n.yamamoto@pwc.com

Korea

Soyoung Park
Partner
s.park@kr.pwc.com

Luxembourg

Vincent Villers
Partner
vincent.villers@lu.pwc.com

Mexico

Fernando Román Sandoval
Partner
fernando.roman@mx.pwc.com

Yonathan Parada
Partner
yonathan.parada@mx.pwc.com

Juan Carlos Carrillo
Director
carlos.carrillo@mx.pwc.com

Middle East

Mike Maddison
Partner
mike.maddison@ae.pwc.com

Netherlands

Gerwin Naber
Partner
gerwin.naber@nl.pwc.com

Otto Vermeulen
Partner
otto.vermeulen@nl.pwc.com

Bram van Tiel
Director
bram.van.tiel@nl.pwc.com

New Zealand

Adrian van Hest
Partner
adrian.p.van.hest@nz.pwc.com

Norway

Lars Fjørtoft
Partner
lars.fjortoft@pwc.com

Eldar Lorezntzen Lillevik
Director
eldar.lillevik@pwc.com

Poland

Rafal Jaczynski
Director
rafal.jaczynski@pl.pwc.com

Jacek Sygutowski
Director
jacek.sygutowski@pl.pwc.com

Piotr Urban
Partner
piotr.urban@pl.pwc.com

Singapore

Tan Shong Ye
Partner
shong.ye.tan@sg.pwc.com

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

Paul O'Rourke
Partner
paul.m.orourke@sg.pwc.com

South Africa

Sidriaan de Villiers
Partner
sidriaan.de.villiers@za.pwc.com

Elmo Hildebrand
Director/Partner
elmo.hildebrand@za.pwc.com

Busisiwe Mathe
Partner/Director
busisiwe.mathe@za.pwc.com

Spain

Javier Urtiaga Baonza
Partner
javier.urtiaga@es.pwc.com

Jesus Manuel Romero Bartolomé
Partner
jesus.romero.bartolome@es.pwc.com

Israel Hernández Ortiz
Partner
israel.hernandez.ortiz@es.pwc.com

Sweden

Martin Allen
Director
martin.allen@se.pwc.com

Rolf Rosenvinge
Partner
rolf.rosenvinge@se.pwc.com

Switzerland

Reto Haeni
Partner
reto.haeni@ch.pwc.com

Turkey

Burak Sadic
Director
burak.sadic@tr.pwc.com

United Kingdom

Zubin Randeria
Partner
zubin.randeria@pwc.com

Richard Horne
Partner
richard.horne@uk.pwc.com

Alex Petsopoulos
Partner
alex.petsopoulos@uk.pwc.com

United States

Sean Joyce
Principal
sean.joyce@pwc.com

David Burg
Principal
david.b.burg@pwc.com

Grant Waterfall
Partner
grant.waterfall@pwc.com

www.pwc.com/gsiss
www.pwc.com/cybersecurityandprivacy

Contributing authors

Christopher Castelli, Barbara Gabriel, Jon Yates,
and Philip Booth