УДК 338

Федишин І.Б.
Тернопільський національний технічний університет імені Івана Пулюя

АНТИКРИЗОВИЙ МЕНЕДЖМЕНТ В ЗАГАЛЬНІЙ ПРОБЛЕМІ ВИРОБНИЧИХ СИСТЕМ

Fedyshyn I.B.

CRISIS MANAGEMENT IN THE GENERAL PROBLEM OF PRODUCTION SYSTEMS

Суспільства стають не тільки більш складними та взаємопов'язаними, але й дедалі більше вразливими щодо впливу непередбачуваних соціальних, економічних та екологічних негативних подій, оскільки нові загрози можуть виникати та швидше поширюватися через ефекти глобалізації. Ця концепція також враховує іншу закономірність нових криз: каскадні ризики, які стають активними загрозами, коли вони поширюються на глобальні системи, незалежно від того, чи виникають вони в галузі охорони здоров'я, клімату, соціальної чи фінансової систем. Підвищена мобільність у глобальному світі сприяє поширенню носіїв ризику чи векторів, таких як віруси чи терористичні атаки. Глобалізація також призвела до посилення взаємозалежності виробничих та постачальницьких систем та їх інфраструктури, а також до централізації та концентрації критичних систем. Ланцюги поставок та мережі життєво важливих служб стають все більш глобальними і тому піддаються багатьом небезпекам та загрозам. Вони також є вразливими, взаємозалежними, і наші суспільства та економіки все більше покладаються на них у своєму щоденному функціонуванні та діяльності. Криза, що зачіпає один вузол такої системи, може вплинути на всю, маючи масштабні каскадні наслідки. Катастрофи виявляють не лише структурні сильні сторони та обмеження середовища певної громади, а й те, як місцеві, державні та національні організації реагування працюють ефективно чи неефективно. Виробникам для збереження конкурентоспроможності доведеться диверсифікувати виробництво згідно з новими стандартами, враховуючи новітні технологічні продукти та процеси, в тому чилі для того, щоб уникнути цінових воєн.

Сьогодні, згідно з Глобальним індексом конкурентоспроможності виробничої сфери, США не посідає перше місце як найконкурентніша економіка світу. Однак перше місце займає Китай. Додатковою макроекономічною змінною, яка може мати серйозні наслідки для світової економіки, є будь-яке уповільнення зростання в Китаї. Китай відіграє важливу роль, завдяки енергійному попиту споживачів (зокрема через розвинену систему Інтернет комерції) та фіскальному стимулюванню, що надається розвиненим країнам Світу за рахунок придбання облігацій та активів. Однак у 2019 році зростання Китаю сповільнилося до приблизно 6% - найнижчий темп його зростання за 30 років, при цьому відбувалося падіння інвестицій, ослаблення внутрішнього попиту та зниження об'ємів експорту (частково через торговельну війну із США). Зростання економіки Китаю, ймовірно, було причиною швидкого відновлення в єврозоні та зростанню, яке спостерігається в США, оскільки навряд чи тільки монетарний стимул міг створити умови для відновлення зростання [1].

Традиційні управлінські та маркетингові зусилля сьогодні для виробників виявляються набагато менш ефективними, ніж у минулому; виставки, торгові оголошення та телефонні опитування вже не працюють так, як раніше. У цифрову епоху організаціям потрібно зробити більше, ніж створити веб-сайт і сподіватися, що їх найкращі перспективи пов'язані тільки з ним. Маркетологи на промислових B2B повиннні докласти зусиль, щоб такий веб сайт можна було органічно знайти через

пошук в Інтернеті, а також надавати велику кількість інформації, яка демонструє актуальність та досвід. Це означає, що потрібно використовувати вхідний маркетинг та тактику SEO, створюючи контент, який дає відповіді на запитання та проблеми потенційних клієнтів.

Надалі, у міру прогресу технологій, зростають зусилля та навички кіберзлочинців. У той час як програмне забезпечення колись було найпоширенішою ціллю кіберзлочинності, після багатьох років бурхливого зростання його обігнали дві "нові" загрози: банківські трояни та криптовалюти (згідно з середньорічним звітом про кібер-атаку «Checkpoint Trend: 2018» [2], кіберзлочинці атакували 42% організацій по всьому світу лише в першій половині 2018 року).

Більшість виробників покладаються на застарілі системи безпеки, нездатні вирішити кількість та складність загроз сьогодні, залишаючись уразливими до атак. Компанії повинні використовувати більш складні способи убезпечення своїх мереж.

Найкраща зброя для боротьби з кібер-атаками - це забезпечення регулярного оновлення всього програмного забезпечення та навчання працівників щодо попереджувальних знаків про порушення безпеки компанії. Один з поширених способів потрапляння кіберзлочинців у мережу - це електронна пошта.

Перше, що необхідно підприємству в кризових умовах - це робота з бізнес-консалтинговою фірмою, яка має досвід у критичних стуаціях.

Ризики, які невідомі через невизначеність впливають на цілі організації та її виживання. Такі ризики можуть призвести до фізичного припинення бізнесу. Ризики цієї категорії включають ризикові події, пов'язані з платоспроможністю, які виникають, коли рішення, прийняті всередині організації або поза нею, мають ефект доміно та впливають на здатність фірми функціонувати.

На відміну від управління ризиками, яке передбачає оцінку потенційних загроз та пошук найкращих способів уникнути цих загроз, управління кризовими ситуаціями передбачає подолання загроз до, під час та після їх виникнення. Управління повинно зосереджуватись відповідно на швидкій, але нетривалій реакції "першої допомоги" та довготривалій фазі відновлення (наприклад, переміщення операцій на інший сайт).

На успішне застосування будь-якої теорії чи концепції як для менеджменту, так і для повсякденного (оперативного) управління сильно впливає ситуація. Наприклад, функціональна організаційна структура з багатьма шарами управління функціонує найкраще в стабільних умовах та рутинних операціях. Для практичного управління операційне середовище повинно бути гнучким, щоб швидко та адекватно реагувати на різноманітні небезпеки, з якими стикається громада чи бізнес. Керівники повинні будувати організаційну культуру та структуру, яка імпровізує та визнає, що кожна криза є унікальною. Як результат, система може бути структурована більш динамічно, виходячи з характеру проблеми (небезпеки) та того, хто потребує участі у прийнятті рішень та вжитих дій. Використання жорсткої структури незалежно від ситуації, може не забезпечити належну основу для швидкого та всебічного прийняття рішень в умовах кризи. А також нові технології, закони та нормативні акти, потреби громади та бізнесу, є основними чинниками, що підштовхують зміни в програмах реагування та відновлення, інструментах планування та підходах до менеджменту взагалі.

Список використаних джерел:

1. Financial Risks in Europe: The End of the Beginning 2020. URL: file:///C:/Users/user/Desktop/QA0420079ENN.en.pdf

2. Check Point Cyber Attack Trends: Mid-Year Report 2018. URL: https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf