

ОЛЕГ ЧОР: Характер економіки диктує те, що треба захищати

Конкуренція, поза сумнівом, є найпотужнішим рушієм економіки. Однак, недобросовісної конкуренції ця фраза аж ніяк не стосується.

Кожна успішна компанія має свої секрети. Це якісь нові технології, бази даних, плани розвитку бізнесу і т.д. Це те, що надає компанії конкурентних переваг. Проте, якщо конкурент у якийсь спосіб дізнається про ваші козирі, переваги з'являться у нього і йому вже нічого не вартуватиме використати проти вас ваші ж секрети. Тому від того, як ви вмієте оберігати свої таємниці залежить ваша доля на ринку.

Про це розповідає віце-президент міжнародного охоронного холдингу «Група Секьюрті» (Канада) Олег Чор.

Промисловий шпигунство в Україні: міф чи реальність? Наскільки актуальною є проблема і на яких рівнях вона є актуальною?

Промислове шпигунство (ПШ) виникло ще з того моменту, як з'явилося поняття об'єднання людей. Племена вже тоді намагалися вкрасти одне в одного технології видобутку вогню, полювання, приготування їжі. Відтак, першими промисловими шпигунами були ще первісні люди.

ПШ в Україні – це, безумовно, реальність. Якби це було не так, великі корпоративні структури не витрачали б на власну безпеку шалені гроші. Найпростіший приклад ПШ – це спроба вкрасти інформацію, отримати доступ до клієнтської бази конкурентів, здобути перелік цін на послуги або отримати інформацію про ціни конкурентів напередодні тендеру.

Робота з персоналом. Як унебезпечитися від витоку цінної інформації від своїх?

На мою думку, лише комплексний підхід може дати результат. Це має бути система – від моменту прийому на роботу до вчасної виплати зарплатні. Треба враховувати цілу низку різних нюансів. Наприклад, далеко не для всіх гроші є основним мотиватором. Для когось це може бути, наприклад, влада або страх.

Наша компанія наприклад розробила цілий комплекс заходів, з допомогою котрого можна захиститися від промислового шпигунства. Якщо говорити про базовий комплект, то тут кілька основних кроків. Щонайперше – правильний підбір, виявлення людей, котрі здатні все продавати. По-друге, постійна і системна робота з персоналом: чітке розмежування рівня доступу залежно від робочих потреб кожного співробітника, чітко складені і контрольовані інструкції – що можна і чого не можна, включаючи порядок зберігання та доступ до документів і інформації, доступ до кабінетів перших осіб компанії. До цього додається цілий комплекс заходів профілактичного характеру, які розробляються для конкретного підприємства з врахуванням його спеціалізації.

Як діють промислові шпигуни? Розкажіть будьласка, про найбільш типові схеми, пов'язані із власним персоналом компанії.

Як це виглядає? – На момент прийому працівника на роботу треба точно зрозуміти психологічний портрет кандидата, а не лише рівень його кваліфікації. і йдеть-

ся не тільки про психологічні тести. Та ж трудова книжка може Вам чимало розповісти – зокрема кількість місць праці даної особи і причини їх зміни. Свого часу в спецслужбах було таке поняття як схильність людини до зради. У кожної людини є своя межа стосовно того, що можна собі дозволити і чого собі дозволяти не можна. Відтак, дуже важливо виявити цю межу даної конкретної людини ще на етапі прийому на роботу. Є люди, які апріорі працюють виключно на себе. Вони, можливо, й не чули про Макіавеллі, однак свято сповідають принцип: «Всі засоби, які служать меті – допустимі». Якщо кінцевою метою є самозбагачення за будь-яку ціну, то треба замислитися над рівнем допуску, не зважаючи навіть на високі професійні якості. А надалі-контроль його роботи.

Якщо говорити про мотив влади, то вважаю, що гарний спеціаліст цілком здатний це визначити. Чи небезпечно це? – Певною мірою, так, якщо амбіції людини збудовані на комплексах. Комплекси Гітлера базувались на тому, що його не визнавали свого часу к художника, а В. Ульянов – на тому, що як юрист він не виграв в суді жодної справи. А першим відомим історії став Герострат, котрий не спромігшись цю створити, вирішив прославитися тим, що спалив храм Артеміди. Людина такого типу, яка не здатна забезпечити високі продажі, може самоствердитися за рахунок того, що завдасть компанії великої шкоди. Мовляв, «От ви думали, що я ні на що не здатен – ось вам, маєте!»

Тут треба пам'ятати про елементарні правила. Одним із успіхів радянської розвідки колись став доступ до найсекретнішої інформації в офісі прем'єр-міністра Індії. Насправді за дуже смішні гроші наші колеги завербували дрібною клерка, який всього-навсього регулярно приносив їм використані копії з друкарських машинок секретарок. Згідно посади у нього не було доступу до секретної інформації, але був доступ до сміття. Як результат, в Москві знали про все, що друкувалося в офісі прем'єр-міністра.

Нині, певна річ, копійок немає. Однак є чернетки у смітниках. Питання в тому, чия рука писала ці чернетки. Особливо, якщо йдеться про президента компанії чи його замів. Колись у Вашингтоні і в Москві були певні групи спеціалістів, які ретельно сортували сміття американського чи радянського посольств.

Відкати. Це взагалі бич України. Як можна цьому протидіяти?

Тут, мабуть, справа не лише в маленьких зарплатах. В Північній Америці сикхів беруть на роботу в контролюючі органи, оскільки не існує зареєстрованих випадків хабарництва серед цих людей. Це релігія, культура, історія, загалом все, що формує менталітет нації. Рівень корупції в Канаді значно нижчий, аніж у США, хоч вони сусіди і рівень життя приблизно однаковий. Тому все це визначається не лише економічним фактором. Для боротьби з цим злом потрібен комплексний підхід.

Це система контролю закупівель в сукупності з високим рівнем матеріального стимулювання служби безпеки. Той хто економить на безпеці, потім розплачується за її відсутність.

Ми вже говорили про підбір персоналу. Так от, це і є найсерйозніше питання – підбір працівників служби безпеки і система субординації. Начальник служби безпеки є одним із найбільш високооплачуваних співробітників компанії і при цьому не підпорядковується нікому, окрім першої особи в компанії. У тих випадках, коли керівник компанії і її власник – це дві різні людини, то підпорядкуватися начальнику служби безпеки має виключно власнику бізнесу. Це моє глибоке переконання.

Звільнення співробітника, який мав доступ до секретної інформації – як уберегти інформацію від «шкідництва», «зливу» інформації з його боку?

В кожному випадку треба вирішувати індивідуально, виходячи з психологічного портрету працівника, якого звільняють (чи він звільняється). В будь-якому випадку все має бути законно.

Ступінь вигоди і ризику від прийому працівника, який прийшов до вас з базами і інформацією від конкурента? – Де гарантія, що він завтра не продасть вашу базу? З іншого боку потрібно розуміти мотивацію чому він пішов. Далеко не завжди у співробітника, що звільняється є корисний мотив. Можливо, неправим був якраз роботодавець і це не значить, що та ж історія повториться з вами. Треба зрозуміти мотивацію працівника. Дружина дізналася, що чоловік закрутив роман із секретаркою і зруйнувала бізнес. Людині обіцяли – і не заплатили... Не йдеться про те, що каже сам працівник, завдання спеціаліста – виявити. Гроші, страх, любов, заздрість, влада – це основні мотиви людської поведінки. Спробуй знайти.



Group 1 Security

Урловская, 38а, офіс 269
Телефон: **(044) 593-4-911**
Моб.: **067 236-16-96**
Cubc-canada@hotmail.com
www.Group1.com.ua