Jaką wartość ma informacja o klauzuli ŚCIŚLE TAJNE ?

Szpiegostwo to przestępstwo polegające na zbieraniu informacji stanowiących tajemnicę państwową i przekazywaniu ich organom innego kraju.
Oprócz szpiegostwa politycznego i wojskowego, często prowadzone jest szpiegostwo gospodarcze w celu zdobycia tajemnic dotyczących technologii produkcji i rozwiązań technicznych danego przedsiębiorstwa.
O ile zasady ochrony informacji stanowiących tajemnicę państwową regulują zapisy ustawy z dnia 5 sierpnia 2010r. O OCHRONIE INFORMACJI NIEJAWNYCH, o tyle ochrona przed szpiegostwem gospodarczym nie jest chroniona zapisami żadnych przepisów.
Dla głębszego zobrazowania tematu spróbujmy porównać „wartość" informacji niejawnej w porównaniu do wartości pieniężnych. I tak według obowiązujących przepisów:

1. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne Dz.U.2011.271.1603

§ 3.

1. Materiał o klauzuli „ściśle tajne" lub „tajne" jest przewożony przez przewoźnika, o którym mowa w § 2 ust. 1 pkt 1-3.
/1) poczta specjalna podlegająca ministrowi właściwemu do spraw wewnętrznych, działająca w jednostkach organizacyjnych Policji, zapewniająca przewóz materiałów na terytorium Rzeczypospolitej Polskiej;
2) komórka organizacyjna urzędu obsługującego ministra właściwego do spraw zagranicznych, zapewniająca przewóz materiałów za granicę i poza granicami Rzeczypospolitej Polskiej pomiędzy urzędem obsługującym ministra właściwego do spraw zagranicznych i jednostkami organizacyjnymi podległymi lub nadzorowanymi przez tego ministra, zwanymi dalej „placówkami zagranicznymi;
3) właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub Szefowi Kontrwywiadu Wojskowego;/

§ 9.

Przesyłki przewozi się w zamkniętej paczce, worku lub innego rodzaju pojemniku, zwanych dalej „pojemnikiem", na którym zamieszcza się pouczenie o postępowaniu w przypadku jego znalezienia.

§ 12.

1. Przesyłkę zawierającą informacje niejawne o klauzuli „ściśle tajne" przewozi i ochrania konwój złożony co najmniej z dwóch

uzbrojonych w broń palną konwojentów posiadających odpowiednie poświadczenia bezpieczeństwa.
2. Przesyłkę zawierającą informacje niejawne o klauzuli „tajne" przewozi i ochrania co najmniej jeden uzbrojony w broń palną konwojent posiadający odpowiednie poświadczenie bezpieczeństwa.
3. Przesyłkę zawierającą informacje niejawne o klauzuli „poufne" lub „zastrzeżone" przewozi i ochrania co najmniej jeden konwojent posiadający odpowiednie poświadczenie bezpieczeństwa lub upoważnienie.
4. Wymóg posiadania broni palnej nie dotyczy przesyłek przewożonych za granicę i poza granicami Rzeczypospolitej Polskiej, a także przypadków, gdy przesyłka jest przekazywana bez pośrednictwa przewoźnika od nadawcy do adresata lub na terenie tej samej miejscowości.
5. Konwojentów wyposaża się w środki łączności umożliwiające kontakt z nimi podczas przewozu oraz zapoznaje się z zasadami postępowania z ochranianymi i przewożonymi przesyłkami.

2. ROZPORZĄDZENIE Ministra Spraw Wewnętrznych i Administracji z dnia 07.09.2010 roku w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne Dz.U.2016.793

§ 9.

1. Konwojowany transport wartości pieniężnych jest chroniony co najmniej przez:
1) jednego konwojenta - przy transporcie wartości pieniężnych powyżej 1 do 8 jednostek obliczeniowych, z zastrzeżeniem § 7 ust. 2;
2) dwóch konwojentów - przy transporcie wartości pieniężnych powyżej 8 do 24 jednostek obliczeniowych;
3) trzech konwojentów - przy transporcie wartości pieniężnych powyżej 24 do 50 jednostek obliczeniowych;
4) czterech konwojentów - przy transporcie wartości pieniężnych powyżej 50 jednostek obliczeniowych.

Tablica 5 – Pojemniki specjalistyczne

Klasa	Wymagania techniczne	Limit wartości pieniężnych w jednym pojemniku (w jednostkach obliczeniowych)
„A"	Pojemnik zamykany co najmniej jednym zamkiem kluczowym lub szyfrowym, wyposażony w system paralizatora lub inny system zabezpieczający	0,3
„B"	Pojemnik zamykany co najmniej jednym zamkiem kluczowym lub szyfrowym, wyposażony w system paralizatora oraz system sygnalizacji akustycznej lub dymnej	0,5
„C"	Pojemnik zamykany co najmniej dwoma zamkami kluczowymi lub szyfrowymi, wyposażony w system paralizatora i system uszkadzania banknotów oraz system sygnalizacji akustycznej lub dymnej	1
„D"	Pojemnik zamykany dwoma zamknięciami klasyfikowanymi według PN-EN 1303:2007/AC 33 w poz. 7 klasa „6" i w poz. 8 klasa „2" oraz odporny co najmniej przez 6 minut na manipulacje (lub inny równorzędny), wyposażony co najmniej w system sygnalizacji akustycznej lub dymnej i system uszkadzania papierowych wartości pieniężnych, których zadziałanie następuje po zdalnym zainicjowaniu w dowolnym czasie albo automatycznie po czasie określonym przez wytwórcę lub w mieszczącym się w tym czasie wyznaczonym limicie czasowym, przeznaczonym na przeniesienie pojemnika do odbiorcy. Próba włamania w dowolnym czasie oraz upływ wyznaczonego limitu czasowego powoduje zadziałanie systemu, w wyniku czego nastąpi uszkodzenie papierowych wartości pieniężnych z zachowaniem możliwości ich identyfikacji	2
„E"	Pojemnik zamykany dwoma zamknięciami klasyfikowanymi według PN-EN 1303:2007/AC w poz. 7 klasa „6" i w poz. 8 klasa „2" oraz odporny co najmniej przez 6 minut na manipulacje (lub inny równorzędny), wyposażony co najmniej w system sygnalizacji akustycznej lub dymnej i system uszkadzania papierowych wartości pieniężnych oraz system lokalizacji pojemnika, których zadziałanie następuje po zdalnym zainicjowaniu w dowolnym czasie albo automatycznie po czasie określonym przez wytwórcę lub w mieszczącym się w tym czasie wyznaczonym limicie czasowym, przeznaczonym na przeniesienie pojemnika do odbiorcy. Próba włamania w dowolnym czasie lub po upływie wyznaczonego limitu czasowego przeznaczonego na przeniesienie pojemnika do odbiorcy powoduje zadziałanie systemu, w wyniku czego nastąpi uszkodzenie papierowych wartości pieniężnych z zachowaniem możliwości ich identyfikacji	4

jednostka obliczeniowa – 120-krotność przeciętnego wynagrodzenia w poprzednim kwartale, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski", na podstawie art. 20 pkt 2 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2015 r. poz. 748, 1240, 1302 i 1311);

Spróbujmy porównać „wartość" informacji niejawnych o klauzuli „ściśle tajne", które przewozi i ochrania konwój złożony co najmniej z dwóch uzbrojonych w broń palną konwojentów z taką samą „obstawą" dla wartości pieniężnych.
Wg. Komunikatu Prezesa Głównego Urzędu Statystycznego z dnia 13 listopada 2018 r. w sprawie przeciętnego wynagrodzenia w trzecim kwartale 2018 r.
Na podstawie art. 20 pkt 2 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2018 r. poz. 1270) ogłasza się, że przeciętne wynagrodzenie w trzecim kwartale 2018 r. wyniosło 4580,20 zł.
9-24 jednostek obliczeniowych = 4 946 616 zł do 13 190 976 zł
Z porównania wynika, że „wartość" informacji niejawnych o klauzuli „ściśle tajne" wynosi ok. 5-13 mln zł.

Zwróćmy przy tym uwagę, że przewóz „informacji niejawnych” nie wymaga żadnych specjalistycznych pojemników tudzież bankowozów. **Konwojent** w jednym, jak i w drugim przypadku **musi być wyposażony w broń**, co stanowi podstawowy warunek.

Czy kwota 5-13 mln zł jest dla przedsiębiorcy kwotą wysoką? Dla przeciętnego przedsiębiorcy na pewno tak, ale już dla banku czy dla Orlenu, który potrafi wyłożyć na start Roberta Kubicy 100 mln zł, na pewno nie jest to wielka kwota. Dla przedsiębiorstw obracających setkami milionów złotych strata kilku milionów nie jest odczuwalna tym bardziej, że w ramach tzw. „dobrej współpracy” zostanie im zwrócona np. przez bank, pomimo, iż włamania na ich konto dokonano w siedzibie firmy /pani Krysia wychodząc do domu zapomniała wyłączyć komputer/.
Przeciętny przedsiębiorca w takim przypadku nie ma praktycznie szans na odzyskanie utraconych pieniędzy, nawet podczas napadu. Zabezpiecza się na tzw. „swój” sposób nie patrząc na certyfikaty i inne zalecenia niekiedy bzdurnych przepisów, które tak naprawdę jego nie dotyczą.
Jak to robi?
Kupuje najdroższy pojemnik specjalistyczny. Demontuje z niego system uszkadzania papierowych wartości pieniężnych. Doposaża go jednocześnie w wewnętrzny szkielet **wypełniony blachą** tak, aby nie można go było rozciąć np. nożem czy bagnetem i dokonać rabunku na miejscu zdarzenia. Dodatkowo wyposaża pojemnik w GPS /usługa monitorowania 24 godz. na dobę/, a równocześnie przed wyjazdem z gotówką w trasę każdorazowo sprawdza czy ktoś nie doczepił mu do samochodu pluskwy w postaci dodatkowego GPS-u. Pluskwa taka nie jest łatwa do wykrycia, ponieważ nie wysyła ciągłego sygnału, a sprzęt profesjonalny do jej namierzenia też nie mało kosztuje. Nauczony przykrym doświadczeniem nie żałuje na inwestycję, która zapewni bezpieczeństwo jemu i jego dochodom. Nawet nie używając broni, co często wiąże się z utratą czyjegoś życia i wieloma kłopotami z tym związanymi, jest w stanie w dużym stopniu zapobiec utraty swoich „ściśle tajnych informacji”.

Podany powyżej przykład obrazuje ochronę informacji niejawnej w przypadku przełożenia jej na wartość materialną. Dopiero takie porównanie trafia do świadomości osób mających do czynienia z ochroną informacji niejawnych zgodnie z USTAWĄ z dnia 5 sierpnia 2010r. O OCHRONIE INFORMACJI NIEJAWNYCH.

Najsłabszym ogniwem w szeroko rozumianym procesie ochrony informacji jest zawsze człowiek. To od niego przede wszystkim zależy przestrzeganie stosownych procedur, zmiana kluczy szyfrujących /itp./ i ogólne dochowanie tajemnicy. Nie pomogą żadne najlepsze urządzenia zabezpieczające, tudzież wzorcowo opracowane procedury, jeśli personel za nie odpowiedzialny będzie lekkomyślny, nielojalny wobec pracodawcy.

Na nic się zda wydawanie setek tysięcy złotych na systemy kontroli dostępu tudzież „wypasione” depozytory kluczy obsługiwane za zbliżeniem karty do czytnika jeżeli przełożony czy osoba odpowiedzialna nie będzie natychmiast reagowała na naruszenia zgłaszane przez system.
A niestety tak się nie dzieje w większości przypadków. W końcu sygnały te powszednieją i nikt nawet na nie nie reaguje.
Tak samo, jak łatwo obsługuje się wejście do danej strefy dzięki zastosowaniu karty zbliżeniowej, tak samo jeszcze łatwiej jest sczytać dane z tej karty. Prawie każdy pracownik nosi taką kartę na wierzchu w postaci identyfikatora bez żadnego jej zabezpieczenia. Wynosi do domu po drodze odwiedzając wiele miejsc, tudzież korzystając z transportu komunikacji miejskiej. W razie zdarzenia trudno jest udowodnić, czy to rzeczywiście osoba odpowiedzialna była sprawcą.

Większość sekretarek trzyma klucze do biur swych szefów i ich szafek we własnych biurkach (łatwo dostępnych). Większość pracowników przechowuje klucze od szaf (sejfów) we własnych biurkach. Aby sprawę jeszcze bardziej "skomplikować", biurka te są rzadko zamykane.
Wreszcie, większość pracowników klucze służbowe wynosi poza teren firmy lub dysponuje ich duplikatami. Tego typu nawyki i praktyki są **niedopuszczalne**.

Nieco archaiczny, aczkolwiek sprawdzony sposób to prowadzenie rejestru wydanych/pobranych kluczy.

	Wydanie Kluczy					Zwrot Kluczy						
L.p.	Data	Godzina	Klucze	Pobierający klucze	Podpis pobierającego	Data	Godzina	Zdający klucze	Podpis zdającego	Przyjmujący klucze	Podpis przyjmującego	Uwagi
1	2	3	4	5	6	7	8	9	10	11	12	13

W razie jakiegokolwiek zdarzenia mamy wszystkie dane pobierającego klucze do danego pomieszczenia/strefy potwierdzone jego podpisem. Nie ma tłumaczenia „to nie ja, to kolega użył mojego identyfikatora do wejścia” lub jak tłumaczą się posłowie podczas oszustw w głosowaniach. Klucze możemy przechowywać w pudełkach lub torebkach plombowanych za pomocą plomb jednorazowych lub plombowanych za pomocą referentki.


https://www.one1.pl/22-pojemniki-na-klucze

Plombowanie za pomocą plomb jednorazowych wydaje się wygodniejsze, ale UWAGA - istniejące na rynku torebki plombowane za pomocą plomb jednorazowych /strzałkowych/ są podróbkami produktów firmy Envopak i „specjaliści" wykazali, że można je otworzyć nie naruszając plomby. Dlatego też firma Envopak od kilku ładnych lat w swoich produktach stosuje zmienioną komorę plombowniczą, której CHIŃCZYK jeszcze nie podrabia. Tylko oryginalny produkt zapewnia pełnię bezpieczeństwa zaplombowanej zawartości.
Drugim sposobem plombowania zawartości jest popularna wśród służb mundurowych referentka. Jest to rodzaj numerowanej pieczęci przypisanej konkretnej osobie i jednocześnie identyfikująca tę osobę. Nawilżając lekko referentkę np. za pomocą śliny odciskamy ją w plastelinie. Każde jej naruszenie jest widoczne na elemencie plombowanym.

https://www.one1.pl/15-zestawy-plombownicze

Porównując referentkę odciśniętą na drzwiach do pomieszczenia i na pojemniku z kluczami mamy pewność, że ta sama osoba przebywała w pomieszczeniu używając danego kompletu kluczy.
Referentka powinna być grawerowana rylcem, co powoduje, że znaki są wyraziste i lepiej odbijają się w plastelinie niż przy grawerowaniu laserowym. Grawerowanie laserowe bywa tańsze, ale nie daje tak pożądanego efektu.

Sposób plombowania za pomocą referentki wydaje się być najbardziej pewnym sposobem plombowania i jednocześnie identyfikatorem osoby, która tego dokonała. Nie nadaremnie służby mundurowe go stosują z powodzeniem od wielu lat i nie zapowiada się na to, żeby z niego zrezygnowały.

Największą bolączką niemal każdej firmy jest praca po godzinach.
Nie dopuszczamy do sytuacji w której pracownik pracuje po godzinach bez stosownego nadzoru. Powstają wtedy przesłanki do różnych niepożądanych zachowań pracownika: kopiowanie danych, wgląd do dokumentów pozostawionych przypadkowo przez innych pracowników itp. Zaczyna się niewinnie od drukowania pracy magisterskiej dziecka na „wypasionej" drukarce. Udało się? No to możemy spróbować…. Pewnie też się uda.

Rozgrzebywanie śmietniska, odpadków, przeglądanie starych dokumentów, wszystko to dotyczy przeszukiwania śmieci w poszukiwaniu cennych informacji. Uważa się, że jest to metoda numer jeden szpiegostwa gospodarczego i osobistego. Strzępy pozornie bezużytecznych informacji są ze sobą powiązane. Działania antyszpiegowskie mają na celu zredukowanie dostępności do poszczególnych elementów tej układanki. Niszczenie **wszelkich**, niepotrzebnych dokumentów jest pierwszym krokiem w tym procesie.



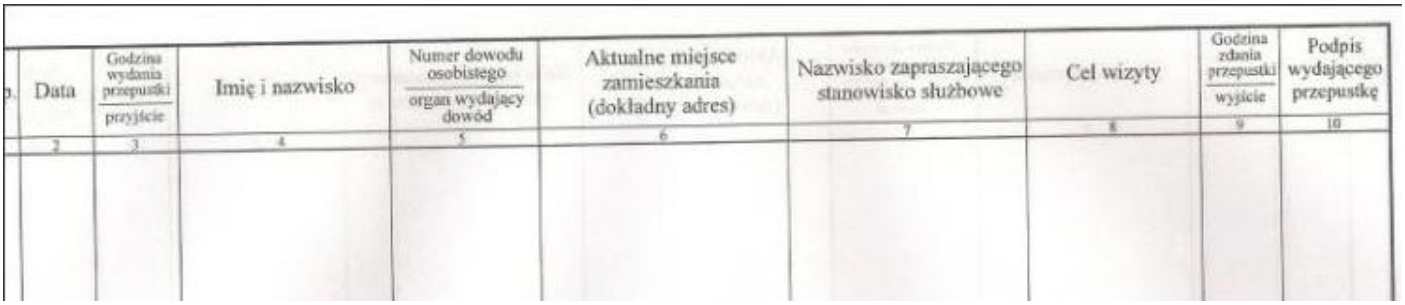
https://www.one1.pl/42-dokumenty-niszczenie

Zalecenia:
- Wymagaj /wyrób nawyk/ od pracowników natychmiastowego niszczenia wszelkich, wyrzucanych dokumentów i materiałów.
- Dokonuj zakupu niszczarek wykonujących wzdłużne i poprzeczne cięcia papieru dla zapewnienia wysokiego poziomu bezpieczeństwa.
- Zakup jednej, dużej niszczarki do wykorzystania przez cały personel jest błędem.

Nie wszyscy będą z niej korzystać, ponieważ niektórzy ludzie są zbyt zajęci, aby spacerować z papierami do niszczarki. Lepszym rozwiązaniem jest zakup kilku mniejszych, podręcznych niszczarek przybiurkowych.
- Nie powierzaj niszczenia dokumentów punktom utylizacji papieru.
Zniszcz je przed przekazaniem do recyklingu.

Często pracownicy pozostawiają w pomieszczeniach różnego rodzaju niezabezpieczone dane typu: poufne dokumenty, skorowidze telefoniczne /które zawierają wszystko oprócz listy płac/, karteczki z hasłami przyklejone do monitora, niezamknięte szafy i biurka, kosze pełne niezniszczonych dokumentów.
Należy uczulić wszystkich, że pomieszczeń biurowych nie pozostawia się otwartych – bez nadzoru. Po zakończonej pracy dokumenty należy schować i zamknąć w sejfach, szafach, biurkach, a dane wrażliwe dodatkowo zabezpieczyć poprzez zaplombowanie. Należy wymóc stosowanie zasady „czystego biurka" po zakończonej pracy.
W pomieszczeniach szczególnie wrażliwych można wręcz wymagać stosowania listy kontrolnej tzw. „check-listy". Błędy popełniają nawet najlepsi. Wystarczy, że mamy gorszy dzień, pokłócimy się z kimś lub nasze dziecko zachoruje, a ryzyko popełnienia błędu drastycznie rośnie. Często winna jest również rutyna. Niestety, w wielu zawodach nie można sobie na błąd pozwolić. Tu z pomocą przychodzi checklista lub inaczej lista kontrolna. **Checklista jest spisem czynności, które powinny być wykonane, najczęściej w odpowiedniej kolejności, gwarantującej optymalny rezultat – szybkość wykonania zadania lub niskie ryzyko błędu.**

Korzystając z usług firmy zewnętrznej na terenie własnego obiektu nie dopuszczaj, aby prace wykonywane były bez nadzoru. Zapewnij obecność osoby, reprezentującej firmę, podczas przebywania osób z zewnątrz na Twoim terenie. Jeżeli to możliwe, dopilnuj aby zakończyli prowadzone roboty w czasie godzin pracy biura. Zewnętrzni wykonawcy robót i ich nieupoważnieni pracownicy nigdy nie powinni mieć możliwości poruszania się bez nadzoru po terenie zawierającym istotne informacje. Należy być szczególnie wyczulonym na dziwne, nadmierne zainteresowanie szczegółami, które nie należą do realizacji zleconego zadania.
Najlepszym sposobem kontroli osób odwiedzających firmę jest zaprowadzenie książki ewidencji gości (przyjścia i wyjścia) wraz z wprowadzeniem systemu przepustkowego.



	Data	Godzina wydania przepustki / przyjście	Imię i nazwisko	Numer dowodu osobistego / organ wydający dowód	Aktualne miejsce zamieszkania (dokładny adres)	Nazwisko zapraszającego stanowisko służbowe	Cel wizyty	Godzina zdania przepustki / wyjście	Podpis wydającego przepustkę
2		3	4	5	6	7	8	9	10


SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU

JEDNORAZOWA KARTA WSTĘPU

Nr 739992

Rok 2015

739992

10:59 12-11 X

ANDRZEJ

TURCZYN

Wstęp do: KANCELARIA SEJMU

Nr pokoju: GOŚĆ PIĘTA

KANCELARIA SEJMU * DZIAŁ PRZEPUSTEK -4- STRAŻ MARSZAŁKOWSKA *

Ciężko w obecnych czasach wyobrazić sobie funkcjonowanie firmy bez telefonu bezprzewodowego lub komórkowego.
Telefony bezprzewodowe i komórkowe są jednymi z najbardziej łatwych celów inwigilacji. Przeciwnie, niż to co się na ogół sądzi, odbiór prowadzonych rozmów jest przeważnie krystaliczne czysty, bez zakłóceń atmosferycznych lub interferencji. Wszystkie słowa łącznie i każde z osobna, są zrozumiałe. Używaj tych urządzeń dyskretnie. Podczas ważnych narad i spotkań bezwzględnie wymagaj ich deponowania przed wejściem do sali obrad.

https://www.one1.pl/25-depozytory

Profesjonalny wykrywacz telefonów komórkowych tudzież podsłuchów kosztuje kilka – kilkanaście tysięcy $. Wszystko poniżej tej ceny to wyroby CHIŃCZYKA. Nie daj się nabrać. Zagłuszacze rzadko zagłuszają sygnały analogowe.

https://www.one1.pl/51-kancelaria-wyposazenie

Szpiegostwo precyzyjnie wymierzone w komputery osobiste, laptopy, sieci komputerowe i zdalnie dostępne porty, jest głównym polem walki.
Podstawowe zabezpieczenie informacji zgromadzonych w systemach komputerowych stanowią hasła. Są one indywidualnymi kluczami do naszych zasobów i narzędzi elektronicznej wymiany informacji. Warto pamiętać o wymyślaniu oryginalnych haseł i częstym ich zmienianiu. Najbezpieczniejsze są długi hasła stanowiące kombinację liter, cyfr i znaków specjalnych, które nie układają się w logiczną całość.
Informacje sklasyfikowane (najważniejsze) przechowujemy w komputerach niedostępnych z sieci zewnętrznej.
Wyjaśnij każdemu, kto posiada wrażliwe informacje w swym komputerze, dlaczego środki bezpieczeństwa są tak ważne. Koszt zastąpienia utraconego sprzętu nie jest jedyną stratą.
Zalecenia:
- Ogranicz fizyczny dostęp do komputerów, ze strony osób trzecich.
- Ogranicz dostęp do oprogramowania. Używaj jakościowych haseł.
- Nigdy nie pozostawiaj aktywnego terminala. Wcześniej zawsze wyloguj się.
- Usuń istotne dane z komputera, na czas kiedy nie jest on używany.
- Odłącz PC od sieci, kiedy jest on nieużywany.
- Wyczyść dyski przed przekazaniem do innych zastosowań.
- Niszcz fizycznie dyski przed utylizacją komputera.
- Nie używaj nieautoryzowanego lub pożyczonego oprogramowania.
- Regularnie twórz kopie zapasowe wszelkich danych.
- Stosuj przenośne nośniki pamięci w formie szyfrowanej.
- Zabroń stosowania prywatnych pamięci USB.
- Zabezpiecz komponenty związane z PC - dyski, kopie zapasowe, etc.
- Zabezpiecz nośniki pamięci: dyskietki i dyski optyczne.
- Komputery, wykorzystujące linie telefoniczne, wymagają dodatkowego zabezpieczenia dostępu.
- Nie prowadź dyskusji na temat systemu bezpieczeństwa z nikim, kogo nie znasz; nie ważne co on Ci będzie opowiadał.

Informacja, jak każdy towar ma swoją cenę. Jej wartość jest uzależniona od kwoty, którą jesteśmy gotowi za nią zapłacić, którą jesteśmy gotowi wydać, aby ją zdobyć. Pewności, że tajemnice firmy są całkowicie chronione nie ma nigdy, jednak zawsze możemy to niebezpieczeństwo minimalizować. Zawsze są firmy i ludzie którzy chcą chronić swoje tajemnice - zawsze są firmy i ludzie którzy te tajemnice chcą zdobyć. Wszystko jest kwestią ceny.

Na zakończenie kilka rad bez specjalnego uzasadnienia, odnoszących się zarówno do właściciela, dyrektora czy też przeciętnego pracownika:

1. Nigdy nie dopuszczaj do stosowania ustawień fabrycznych w żadnych urządzeniach - szczególnie służących do przechowywania dokumentów niejawnych /sejfy/.
2. Nie używaj darmowego oprogramowania antywirusowego.
3. Nigdy nie klikaj na linki przesyłane w wiadomościach email od nieznajomych.
4. Nigdy nie łącz się z bankiem za pośrednictwem telefonu komórkowego.
5. Nigdy nie korzystaj ze zdalnej mobilnej płatności.
6. Nigdy nie korzystaj ze zbliżeniowej mobilnej płatności.
7. Zabezpiecz swoją kartę kredytową przed ewentualnym sczytaniem.
8. W bankowości elektronicznej adres, login i hasło wpisujemy ręcznie za każdym razem /bez wyjątków/.
9. W bankowości elektronicznej staraj się używać listy haseł jednorazowych, jeśli nie masz takiej możliwości to hasła sms odbieraj na innym telefonie /nie na tym z którego korzystasz/.
10. W prywatnym telefonie komórkowym wyłącz wszelkiego rodzaju połączenia z Internetem, pocztą email, komunikatorami itp.