



Systemy zarządzania bezpieczeństwem informacji: co to jest, po co je budować i dlaczego w urzędach administracji publicznej

Wiesław Paluszyński

Prezes zarządu TI Consulting

- Zdefiniujemy bezpieczeństwo informacji
- Jak budować bezpieczeństwo informacji
- Podejście oparte na powszechnie uznawanych normach
- Trzy modele budowania bezpieczeństwa informacji
- Audyt bezpieczeństwa punktem wyjścia do tworzenia polityki bezpieczeństwa
- Jak osiągnąć wyznaczony poziom bezpieczeństwa, a następnie utrzymać w czasie

- Błędne podejście:
 - Pokaż mi ROI
 - To tylko generuje koszty
 - Czy mogę mieć pewność?
 - Transfer ryzyka = transfer odpowiedzialności
 - Bezpieczeństwo informacji = bezpieczeństwo internetowe
 - Bezpieczeństwo to sprzęt, a nie organizacja („twarde”, a nie „miękkie”)
- W rzeczywistości:
 - Model oparty na ryzyku
 - To jest dźwignia biznesu
 - Mogę zmniejszyć ryzyko, ale nie mogę go wyeliminować w 100%
 - Bezpieczeństwo wewnątrz firmy jest największym problemem
 - Bezpieczeństwo to tylko 5% nakładów na informatykę

bezpieczeństwo informacji i systemów teleinformatycznych – wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, niezaprzeczalności, rozliczalności autentyczności i niezawodności informacji i systemów, w których są one przetwarzane.

PN ISO/IEC 17799:2003

PN-I-13335-1:1999

polityka bezpieczeństwa informacji - udokumentowany zbiór zasad, praktyk i procedur, w którym dana organizacja określa, w jaki sposób chroni aktywa swego systemu informatycznego oraz przetwarzane informacje.

PN ISO/IEC 17799:2003

zarządzanie ryzykiem – Skoordynowane działania kierowania i kontrolowania organizacji z uwzględnieniem ryzyka
ISO Guide 73:2002

system zarządzania bezpieczeństwem informacji -
ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji
ISMS - information security management system
PN-I-07799-2:2005

- Jak sformułować wymagania bezpieczeństwa
 - Trzy źródła wymagań bezpieczeństwa
 - Ryzyko dotyczące instytucji (tzw. Business perspective)
 - Zbiór wymagań prawnych, statutowych, regulacyjnych i kontraktowych
 - Specyficzny dla instytucji zbiór zasad, celów i wymagań dla przetwarzania informacji, które już zostały wypracowane
- Szacowanie ryzyka dotyczącego bezpieczeństwa
 - Prawdopodobieństwo zdarzenia i powaga szkody
 - Okresowe powtarzanie przeglądów ryzyka
- Wybór zabezpieczeń
 - Wybór zabezpieczeń ograniczających ryzyko do określonego, akceptowalnego poziomu,
 - Uwzględnianie kosztów wdrożenia w odniesieniu do ograniczanego ryzyka oraz wielkości potencjalnych szkód

- Punkt wyjścia do zapewnienia bezpieczeństwa informacji
 - Najważniejsze zabezpieczenia (prawne):
 - Ochrona danych osobowych
 - Ochrona dokumentów instytucji
 - Prawa własności intelektualnej
 - Najlepsze zabezpieczenia
 - Dokument polityki bezpieczeństwa informacji
 - Odpowiedzialność związana z bezpieczeństwem informacji
 - Edukacja i szkolenia w dziedzinie bezpieczeństwa informacji
 - Zgłaszanie przypadków naruszenia bezpieczeństwa
 - Zarządzanie ciągłością działalności instytucji.

- PN-I-13335-1: 1999 „Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych”
- ISO/IEC TR 13335-2:2003 „Zarządzanie i planowanie bezpieczeństwa systemów informatycznych”
- ISO/IEC TR 13335-3:2003 „Techniki zarządzania bezpieczeństwem systemów informatycznych”
- PN ISO/IEC 17799:2003 „Praktyczne zasady zarządzania bezpieczeństwem informacji”
- PN –I- 07799-2:2005 „Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne stosowania” (przyjęta do ustanowienia we wrześniu 2004; identyczna z BS 7799-2:2002)

- ISO/IEC Guide 73:2002 Risk management — Vocabulary — Guidelines for use in standards
- ISO/IEC 13335-1: 2004 Guidelines for the management of IT Security —Part 1:Concepts and models for information and communications technology security management
- ISO/IEC 17799:2005 „Code of Practice for Information Security Management” (2. wydanie oczekuje na publikację)

Projekty norm:

- ISO/IEC FDIS 27001: „Information security management systems Requirements (w oparciu o BS 7799-2:2002)
- ISO/IEC 1stCD 13335-2: Information technology - Security techniques — Management of information and communications technology security — Part 2: Techniques for information and communications technology security risk management

- Wzrost znaczenia bezpieczeñstwa informacji – konkurencja rynkowa i czynniki zewnętrzne (wejście Polski do UE, globalizacja współpracy gospodarczej)
- Sprawdzone podejście i dobre praktyki przeniesione z przodujących ekonomicznie krajów
- Przeniesienie norm międzynarodowych do systemu normalizacji w Polsce – standardy dla administracji publicznej pilnie poszukiwane
- Gwałtowny wzrost liczby organizacji, które poddały niezależnej ocenie swoje systemy zarządzania bezpieczeñstwem informacji na zgodność z BS 7799-2 lub ich krajowymi odpowiednikami
- Zidentyfikowane potrzeby niezależnej oceny systemów zarządzania bezpieczeñstwem informacji w Polsce

Model III

System zarządzania bezpieczeństwem informacji (ISMS)

Model II

Polityka bezpieczeństwa z elementami ISMS

Model I

ISMS - minimalne wymagania

Metodyki oparte na powszechnie uznawanych normach

- prowadzenia audytu (przeglądu bezpieczeństwa)
- zarządzania ryzykiem
- zarządzania projektem



Dla kogo?

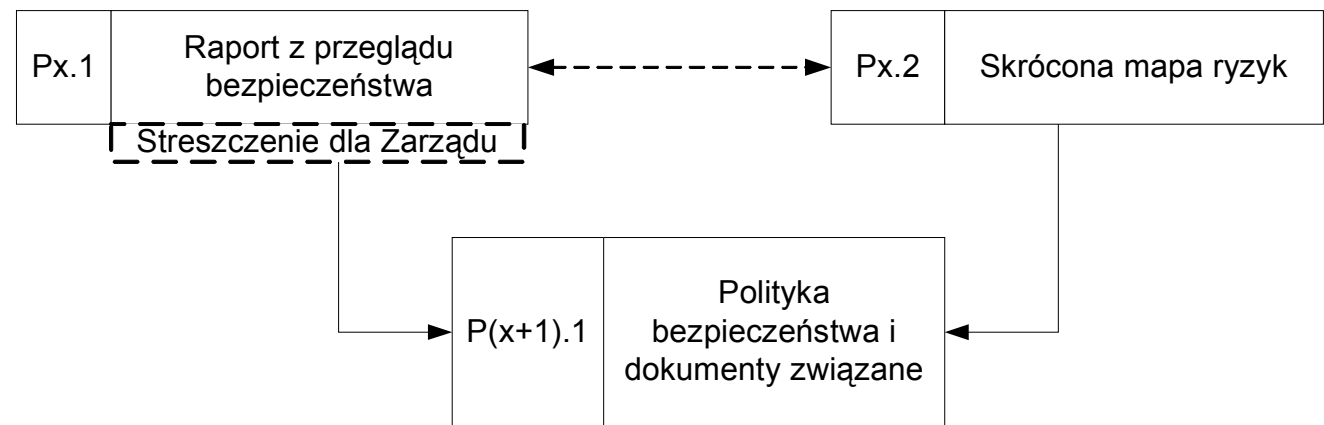
Małe organizacje
Bez polityki bezpieczeństwa

Na czym polega?

Przedsięwzięcie jednorazowe
Minimalne nakłady finansowe

Jaki efekt?

ochrona informacji na zasadzie „działanie doraźne”



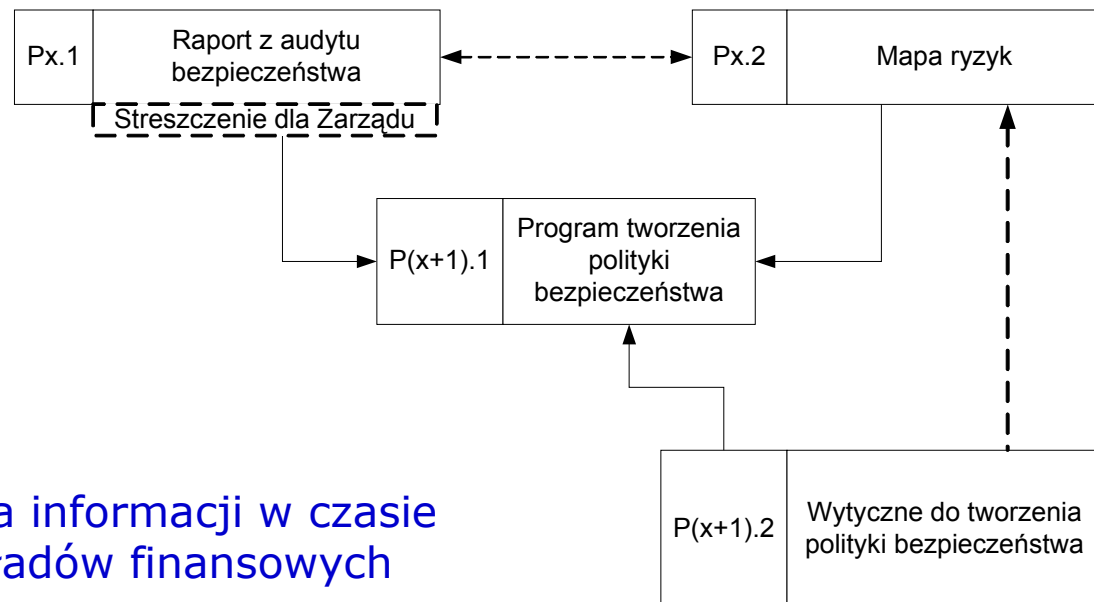
Dla kogo?

Organizacje dowolnej wielkości
Elementy polityki bezpieczeństwa

Na czym polega?

Zarządzanie przez ryzyko
Zarządzanie bezpieczeństwem
(planowanie, wdrażanie, eksploatacja)
Plany i programy bezpieczeństwa, zmiany organizacyjne

Jaki efekt?



Kompleksowa ochrona informacji w czasie
Optymalizacja nakładów finansowych

Dla kogo?

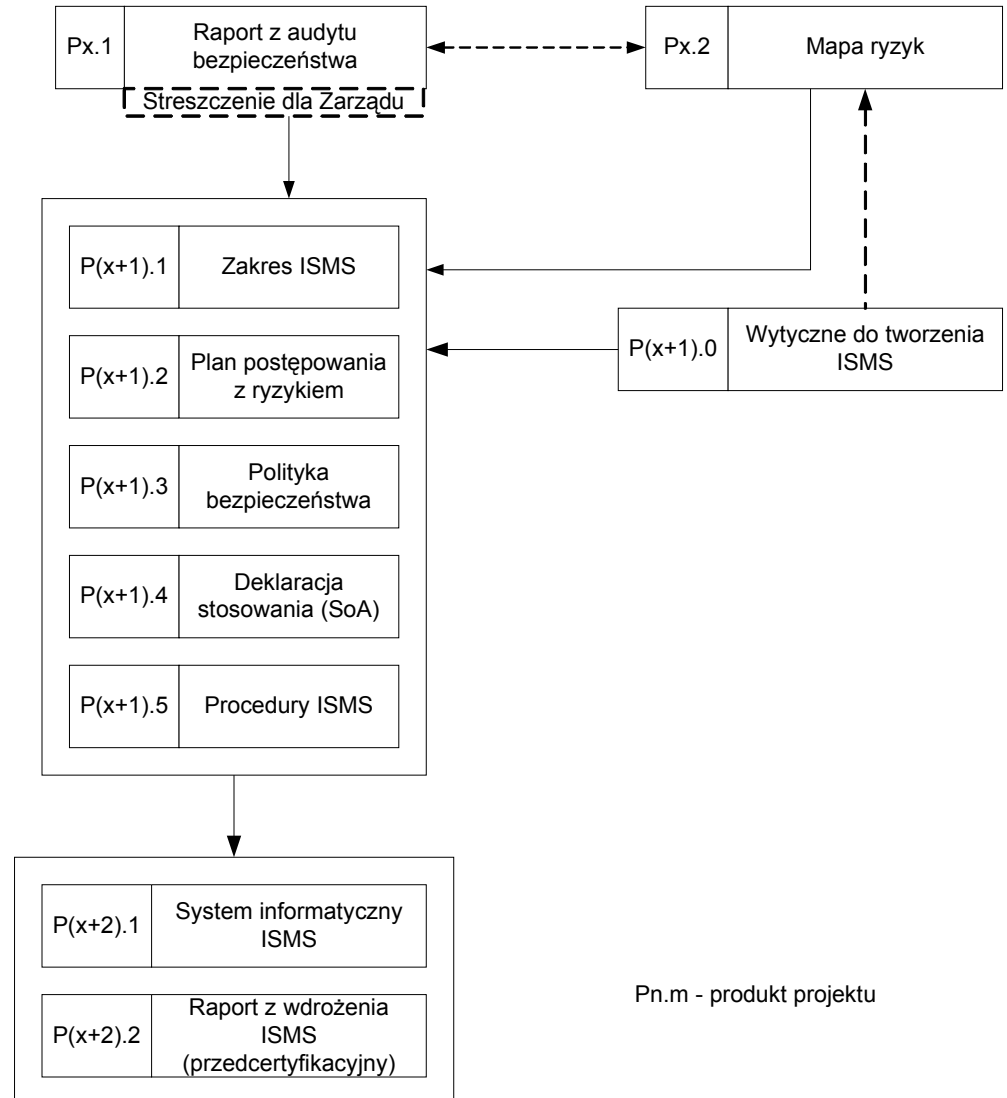
Organizacje dowolnej wielkości
Certyfikat zgodności jako wyróżnik rynkowy
lub wymaganie prawne

Na czym polega?

Zarządzanie przez ryzyko
System zarządzania bezpieczeństwem informacji
w pętli PDCA
Monitorowanie i doskonalenie
systemu zarządzania bezpieczeństwem informacji
Certyfikat zgodności z PN-I-07799-2:2005

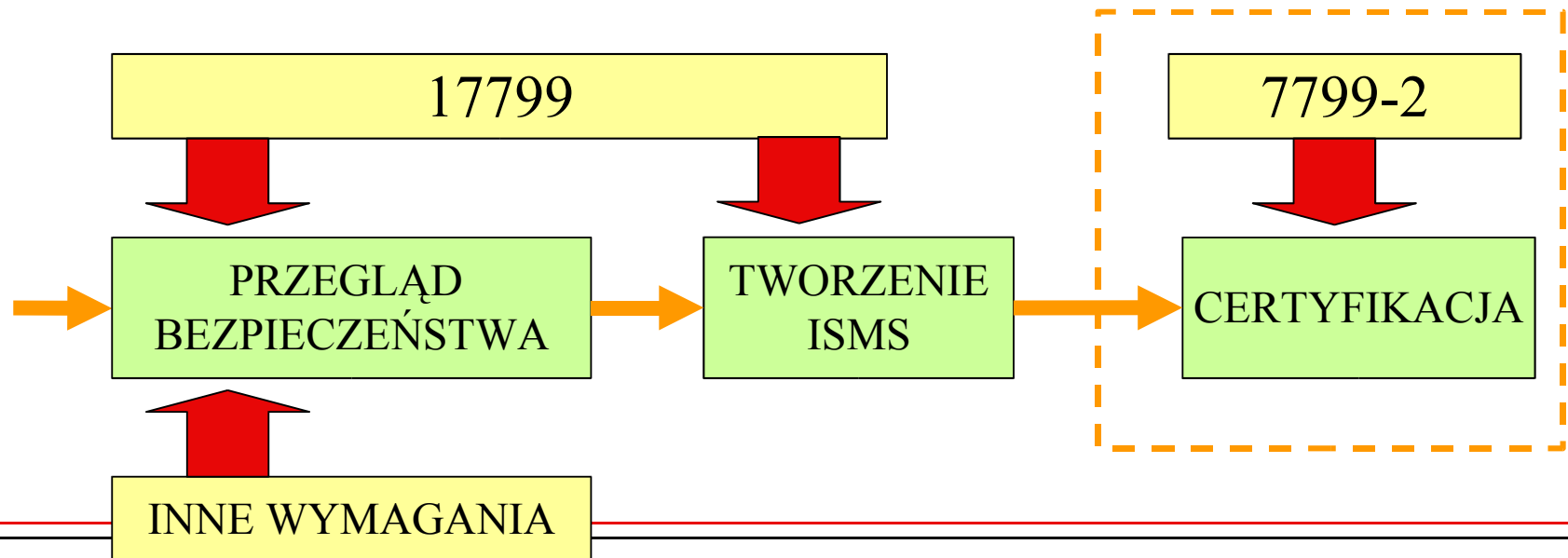
Jaki efekt?

Niezależne poświadczenie
stanu bezpieczeństwa,
Wartość rynkowa
certyfikatu zgodności



Przegląd bezpieczeństwa:

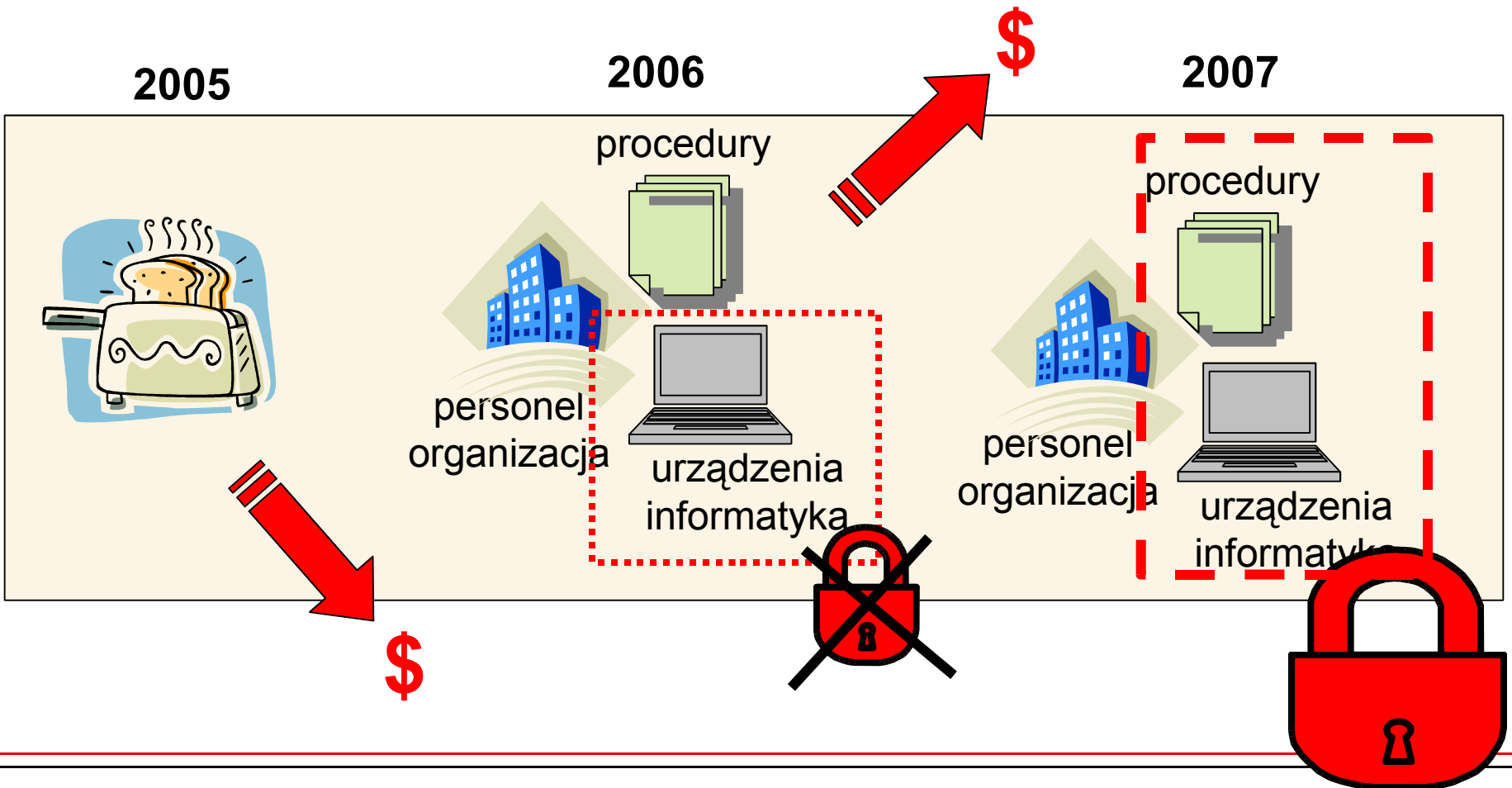
- zgodny z PN-EN ISO 19011
- w oparciu o normę PN-ISO/IEC 17799 – wytyczne dotyczące systemów zarządzania bezpieczeństwem informacji
- Według innych wymagań obowiązujących organizację
 - Prawne
 - Regulaminy wewnętrzne
 - Standardy techniczne





\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$
\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

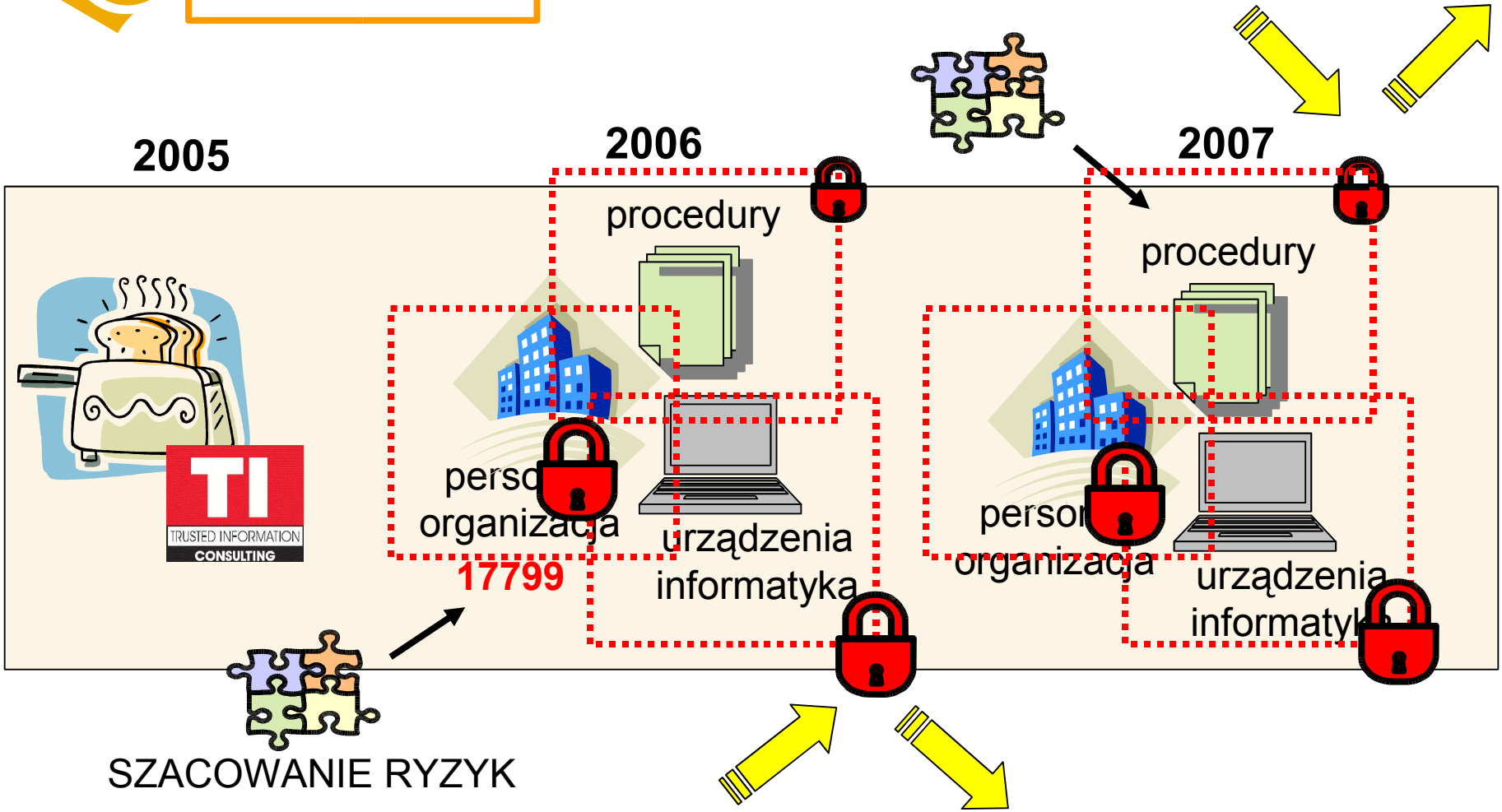
Tak można, ale...





\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$
\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

Tak lepiej!



Proszę o pytania.....



wieslaw.paluszynski@ticons.pl