# LECTURE 12
# RISK TREATMENT

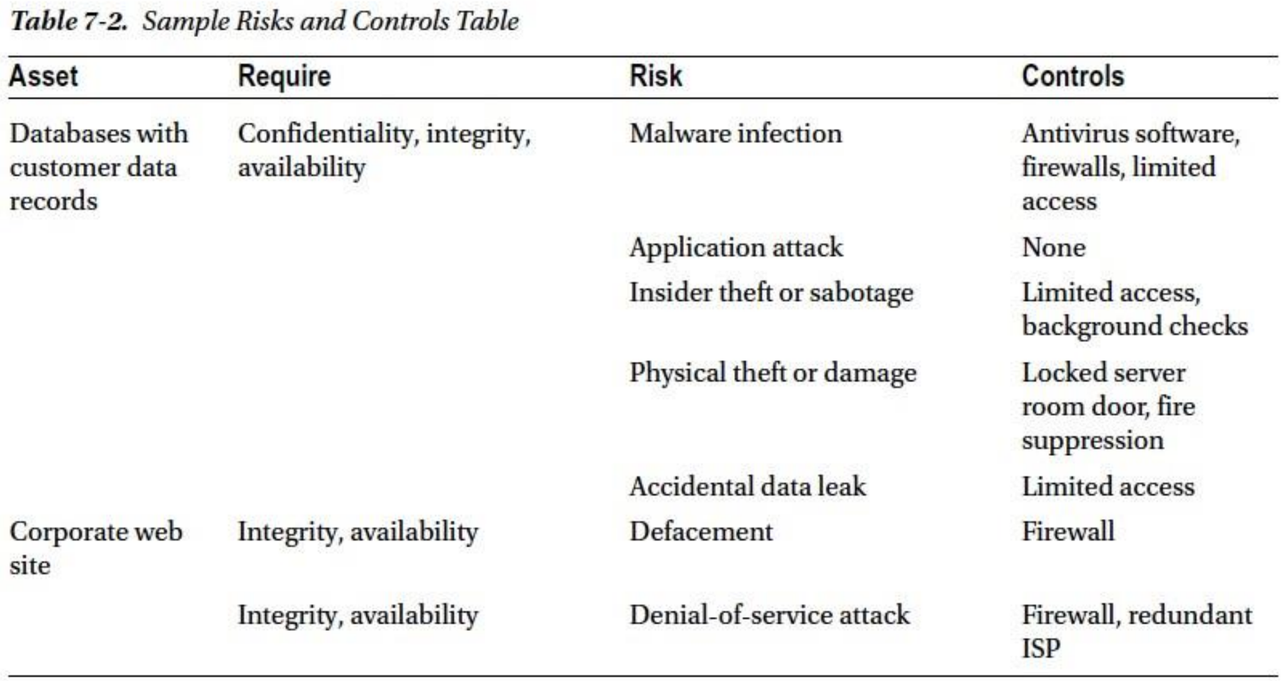
# Topics

- Risk Acceptance
- Risk Elimination
- Risk Reduction
- Risk Transfer

# Introduction

- ✓ You can map risks and control after evaluation phase.
- ✓ Like before, if you haven’t done a risk assessment or a controls analysis, you absolutely need to do them now.

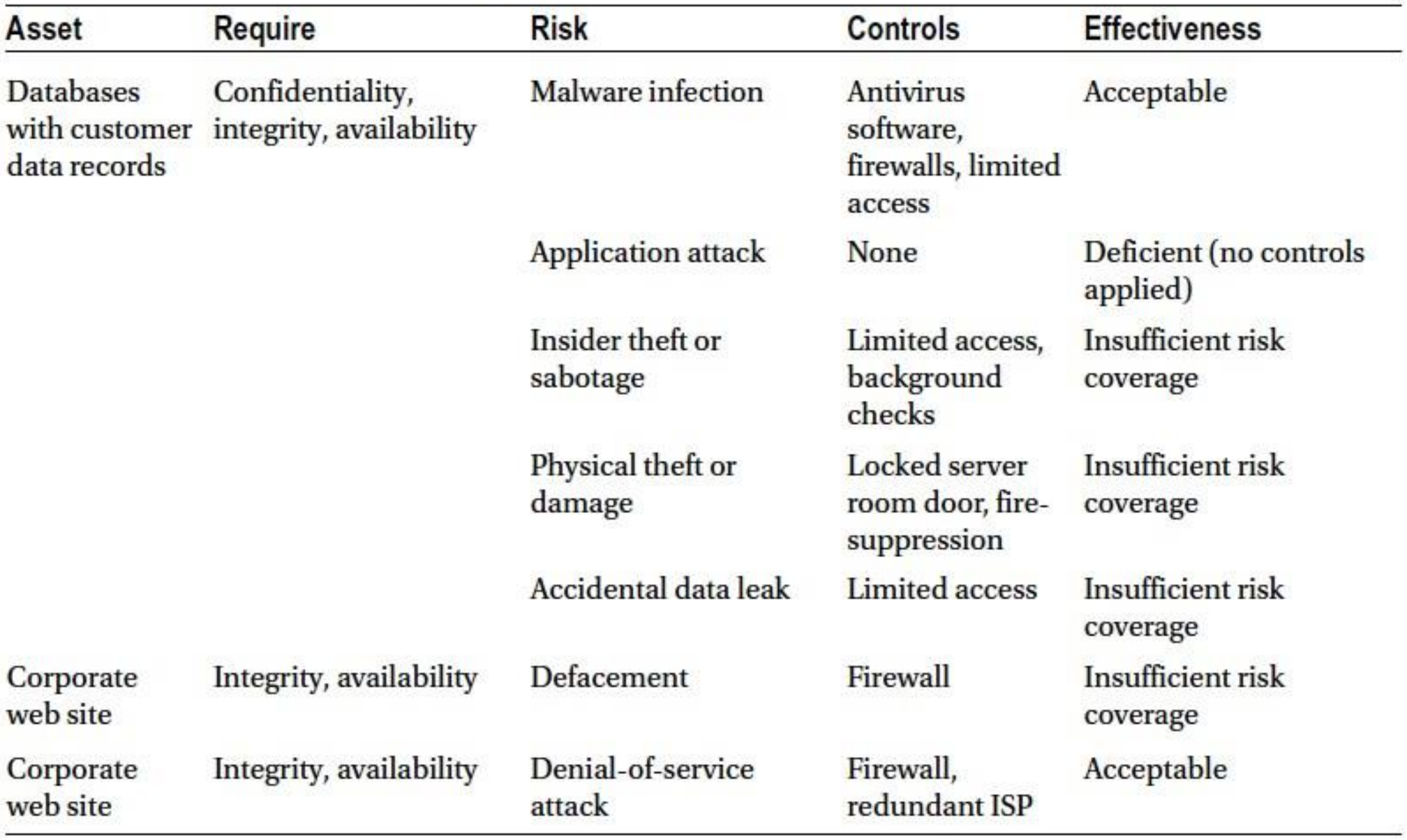
*Table 7-2. Sample Risks and Controls Table*



| Asset | Require | Risk | Controls |
|---|---|---|---|
| Databases with customer data records | Confidentiality, integrity, availability | Malware infection | Antivirus software, firewalls, limited access |
| | | Application attack | None |
| | | Insider theft or sabotage | Limited access, background checks |
| | | Physical theft or damage | Locked server room door, fire suppression |
| | | Accidental data leak | Limited access |
| Corporate web site | Integrity, availability | Defacement | Firewall |
| | Integrity, availability | Denial-of-service attack | Firewall, redundant ISP |

# Introduction

- ✓ After you’ve looked at your risks and current controls, you will likely discover controls that are managing risks insufficiently.
- ✓ They basically have four choices at this point or for risk treatment:
  - *Risk Acceptance*
  - *Risk Elimination*
  - *Risk Reduction*
  - *Risk Transfer*



| Asset | Require | Risk | Controls | Effectiveness |
|---|---|---|---|---|
| Databases with customer data records | Confidentiality, integrity, availability | Malware infection | Antivirus software, firewalls, limited access | Acceptable |
| | | Application attack | None | Deficient (no controls applied) |
| | | Insider theft or sabotage | Limited access, background checks | Insufficient risk coverage |
| | | Physical theft or damage | Locked server room door, fire-suppression | Insufficient risk coverage |
| | | Accidental data leak | Limited access | Insufficient risk coverage |
| Corporate web site | Integrity, availability | Defacement | Firewall | Insufficient risk coverage |
| Corporate web site | Integrity, availability | Denial-of-service attack | Firewall, redundant ISP | Acceptable |

# Introduction

***Why majority organization will not ignore the risk?***

1. ***Organization can be sued and fined for negligence which could defame the organization reputation***

2. ***Reflect that organization fail to do what is reasonable to prevent something bad from happening***

# Risk Acceptance

- ✓ Risk acceptance is the deliberate and carefully considered formal act of declaring that an organization will deal with the consequences of a risk impact.
- ✓ This is not ignorance, where you pretend the problem doesn’t exist.
- ✓ This is a conscious choice, documented in writing, that the risk is acceptable.
- ✓ This is usually done for risks that where the impact or likelihood is small.
- ✓ It can also be done for risks where the cost of managing that risk is higher than the impact.

# Risk Elimination

- ✓ There have been times when an organization did a risk analysis on a particular process and decided to drop that process entirely.
- ✓ The risk could simply be too high and the cost of reducing that risk just not worth it.
- ✓ Maybe the process is not that critical to the organization and in some cases, the organization may find a way to redesign or reorganize the process so the risky functions are no longer performed.
- ✓ Perhaps the process could be folded into another function, and the risk moved that way.
- ✓ In any case, risk elimination means that this particular risky process and its assets are shut down and with them, the associated risk.

# Risk Reduction (With Control)

- This is the most common choice that people make when confronted with risk. It’s likely that your organization is already trying to reduce perceived risks with controls.
- For example, It’s become automatic to install firewalls, passwords, and antivirus for IT systems. It’s a suboptimal solution because the risk is rarely reduced to zero, but it’s the generally accepted solution and is often good enough.

- In the analysis, several risks were not reduced enough by controls:
  - *Application attacks against the database and customer records*
  - *Insider theft or sabotage against the database and customer records*
  - *Physical theft or damage of the database and customer records*
  - *Accidental data leaks of the database and customer records*
  - *Defacements of the corporate web site*

# Risk Reduction (With Control)

- ✓ Often a risk can be reduced by using many different types of controls.
- ✓ It may take some work to determine which control works best in your organization.
- ✓ For example, with the Application attack, risk against the database could be reduced by hardening the software with the programming work done by the developers (as shown in the preceding example).
- ✓ Alternatively, perhaps IT could install an application aware filtering firewall or proxy in front of the database to stop attacks before they get there.
- ✓ For the physical theft risk of the databases, facilities could add better door locks or IT could implement database encryption.

# Risk Transfer

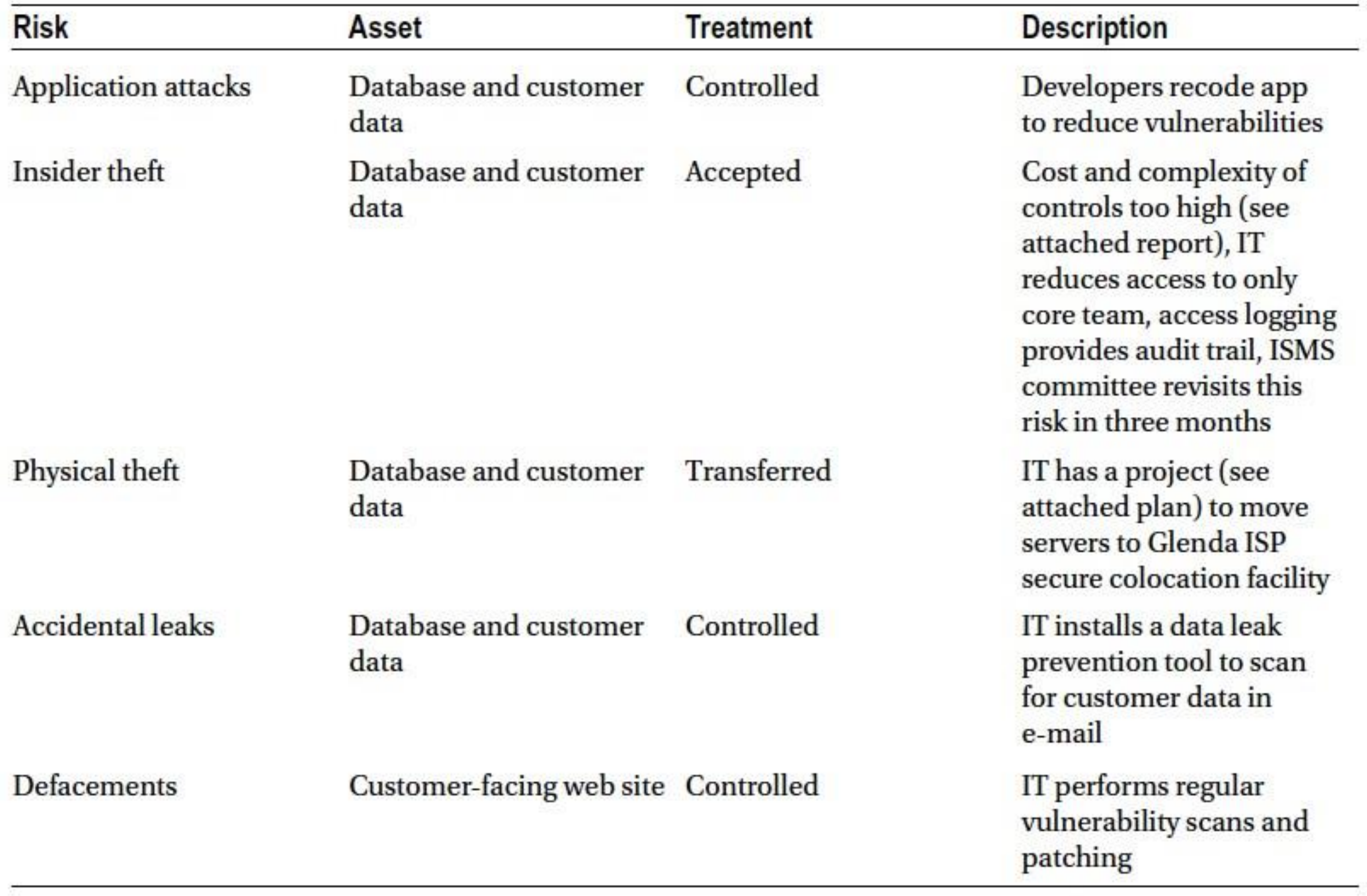
- ✓ There is actually a fifth option, which is a hybrid of risk elimination and risk reduction: risk transfer.
- ✓ For a risk transfer, you transfer either the impact or risky activity itself out of your organization.
- ✓ Many companies choose to outsource their payment card operations for this reason.
- ✓ They haven't fully eliminated the risk, because their customers will still be angry if hackers steal their credit cards.
- ✓ However, the outsourcing company can be contractually bound to pay for the damages if this happens.

# Risk Transfer

- ✓ Another way to transfer risk is to simply buy cyber-insurance against the risk.
- ✓ There were already many insurance options for disaster related IT risks.
- ✓ Now many hacking or data breach risk premiums are available.
- ✓ Be warned however, insurance companies may interpret a covered loss much differently than you might.
- ✓ You should make sure that your policy really covers what you think it does before you consider a risk transferred.

# Documenting Risk Treatment

- ✓ Once all of this done, the ISMS committee should document their proposed risk treatments.
- ✓ For each risk listed, needs to commission a plan.
- ✓ *Why documenting treatment is important?*



| Risk | Asset | Treatment | Description |
|---|---|---|---|
| Application attacks | Database and customer data | Controlled | Developers recode app to reduce vulnerabilities |
| Insider theft | Database and customer data | Accepted | Cost and complexity of controls too high (see attached report), IT reduces access to only core team, access logging provides audit trail, ISMS committee revisits this risk in three months |
| Physical theft | Database and customer data | Transferred | IT has a project (see attached plan) to move servers to Glenda ISP secure colocation facility |
| Accidental leaks | Database and customer data | Controlled | IT installs a data leak prevention tool to scan for customer data in e-mail |
| Defacements | Customer-facing web site | Controlled | IT performs regular vulnerability scans and patching |

## Roadmap/Mind Map