**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 01**

**Risk Management - Contingency Planning Within Information Security**

1. **IT Risk Management and Disaster Recovery**

Kelas ini akan mendiskusikan secara lengkap pengetahuan untuk menilai dan mengembangkan keamanan TI sebuah perusahaan melalui review kebijakan dan pengembangan prosedur. Pemahaman yang mendalam tentang masalah keamanan jaringan, teknik intrusi dan penetrasi karena kerentanan, aplikasi web review dan respon insiden akan didiskusikan pada awal pertemuan di kelas. Prinsip dan alat untuk tindakan pencegahan dalam jaringan, komputer dan forensik jaringan dan aplikasi keamanan sebagai bagian dari manajemen risiko akan dibahas juga . Seperti saat ini infrastruktur TI strategis untuk keberlanjutan bisnis dan pertumbuhan bisnis, oleh karena itu rencana pemulihan bencana menjadi penting dalam sebuah badan usaha. Sebuah pengetahuan yang kuat dari manajemen risiko keamanan harus menjadi bagian dari profesional TI dan tim manajemen. Aspek kelangsungan bisnis akan dibahas karena gangguan infrastruktur akan berdampak parah pada operasional perusahaan.

1. **Risk Management**

Sebagai bagian dari information security, risk management adalah proses untuk mengindentifikasi resiko termasuk ancaman ancaman terhadap kelangsungan bisnis perusahaan dan bagaimana cara mengontrol ancaman ancaman tersebut. Salah satu program dari risk management adalah pembuatan dan penerapan contingency planning. Sebelum berbicara contingency planning secara lebih dalam, maka harus dipahami dulu konsep risk management.

Proses untuk mengindentifikasi risk dan mengontrol risk yang mungkin akan terjadi disebut risk management. Pada gambar 1, di tunjukkan dengan lebih jelas bagian bagian dari risk manajemen, yaitu:

* **Risk Identification**:
  + Process untuk mengindentifikasi dan membuat dokumen tentang semua ancaman yang mungkin terjadi. Selanjutnya pada tahap ini juga dilakukan risk assessment, yaitu sebuah proses untuk memilah milah mana ancaman yang sangat berpotensial untuk merugikan dan mana yang kemungkinan kecil dapat terjadi.
* **Risk Control**:
  + Proses untuk mengontrol ancaman ancaman sehingga dapat mengurangi atau menghilangkan akibat dari ancaman ancaman terhadap informasi.

Pada dasarnya IT risk management ini mempunyai filosofi dari seorang ahli perang dari china yaitu jendral Sun Tzu, beliau mempunyai konsep seperti dibawah ini:

*If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.*

Pada filosofi diatas, apabila kita mengetahui kekuatan dan kemampuan musuh serta mengetahui kekuatan dan kemampuan kita sendiri maka kita dapat memprediksi resiko yang akan terjadi. Jika kita tidak mengetahui kekuatan lawan dan hanya mengetahui kekuatan dan kemampuan kita sendiri maka kemungkinan kita dapat mendapatkan kerugian dari resiko yang tidak kita ketahui. Adalah sangat berbahaya bila kita tidak mengetahui kekuatan musuh dan juga tidak mengetahui kekuatan kita sendiri.

**Know yourself:**

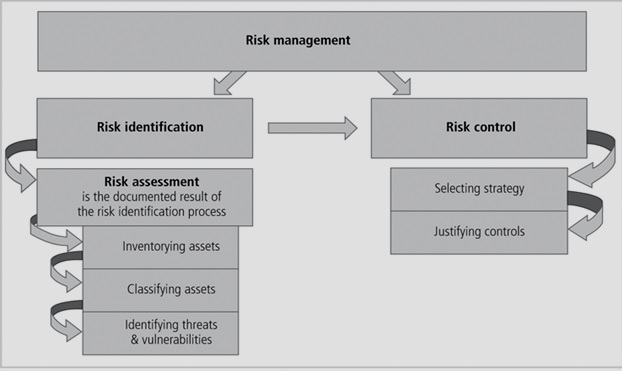
Untuk mengetahui kekuatan dan kemampuan diri kita sendiri maka yang harus dilakukan adalah:

* Identifikasi semua data dan informasi yang ada di tempat kita bekerja
* Lakukan analisa terhadap semua data dan informasi tersebut
* Pahami benar benar aliran data dan informasi tersebut
* Identifikasi asset, yaitu semua hardware dan software yang digunakan untuk menyimpan, memproses dan mengirimkan data atau informasi.
* Dalam melakukan analisa, dapat dipikirkan dengan menjawab pertanyaan sebagai berikut:
  + Bagaimana asset tersebut menjadi bernilai terhadap perusahaan
  + Apa saja kelemahan dari pada asset tersebut
  + Berapa lama sekali asset tersebut perlu diganti, atau di maintain
  + Apakah sudah ada control terhadap asset asset tersebut?

**Know the enemy atau resiko:**

Untuk mengetahui kekuatan dan kemampuan resiko atau enemy maka yang harus dilakukan adalah:

* Identifikasi semua ancaman yang ada di tempat kita bekerja
* Lakukan analisa terhadap semua ancaman atau resiko tersebut
* Pahami benar benar scenario ancaman tersebut
* Identifikasi control yang ada terhadap semua ancaman yang ada.
* Identifikasi juga mitigation strategic, termasuk biaya yang timbul dan keefektifannya

 Gambar 1. Bagian bagian dari risk manajemen (diambil dari Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery, chapter 1.)

**SIMPULAN**

Hal utama dalam IT Security dan IT Risk Management adalah:

1. Indentifikasi Risk
2. Indentifikasi Threat dan ancaman
3. Indentifikasi Control