NAMA : Mohammad Fahman .F

NIM : 1310651177

MK : KEAMANAN INFORMASI

KELAS : TI-A

Domain 3: Informasi

Tata Kelola Keamanan dan

Manajemen Risiko 3

TUJUAN UJIAN DALAM BAB INI

A. ANALISIS RISIKO

Semua profesional keamanan informasi menilai risiko: kita melakukannya begitu sering sehingga menjadi sifat kedua. Analisis Risiko akurat adalah keterampilan penting untuk keamanan informasi profesional. Kita harus menahan diri untuk standar yang lebih tinggi ketika menilai risiko. Kami keputusan risiko akan menentukan yang pengamanan kita menyebarkan untuk melindungi aset dan jumlah uang dan sumber daya yang kami habiskan melakukannya. Keputusan yang buruk akan menghasilkan di buang uang atau, bahkan lebih buruk, data dikompromikan.

B. Aktiva

Aset adalah sumber daya berharga Anda mencoba untuk melindungi. Aset dapat data, sistem, orang, bangunan, properti, dan sebagainya. Nilai atau kekritisan aset akan menentukan

apa pengamanan Anda menyebarkan.

C. Ancaman dan kerentanan

Ancaman adalah segala sesuatu yang berpotensi dapat menyebabkan kerusakan pada aset. ancaman termasuk

gempa bumi, listrik padam, atau cacing berbasis jaringan.

Kerentanan adalah sebuah kelemahan yang memungkinkan ancaman untuk menyebabkan kerusakan. Contoh kerentanan (pencocokan ancaman kami sebelumnya) yang bangunan yang tidak dibangun untuk menahan gempa bumi, pusat data tanpa daya cadangan yang tepat, atau Microsoft Windows Sistem XP yang belum ditambal dalam beberapa tahun.

Risiko = threat3vulnerability

Untuk memiliki risiko, ancaman harus terhubung ke kerentanan. Hubungan ini dinyatakan oleh

rumus:

Risiko ¼ threatvulnerability

Anda dapat menetapkan nilai untuk risiko tertentu menggunakan formula ini. Menetapkan nomor untuk kedua ancaman dan kerentanan. Kami akan menggunakan berbagai 1-5 (rentang adalah sewenang-wenang; hanya terus konsisten ketika membandingkan risiko yang berbeda).

Dampak

The **"risk¼threatvulnerability"** Persamaan kadang-kadang menggunakan variabel tambahan yang disebut Dampak: ". risk¼threatvulnerabilityimpact" Dampak adalah keparahan kerusakan, kadang-kadang dinyatakan dalam dolar. Risk¼threatvulnerabilitycost kadang-kadang digunakan untuk alasan itu. Sebuah sinonim untuk dampak adalah konsekuensi.

D. Matrix Analisis Risiko

Table 3.1 Risk Analysis Matrix

		Consequences				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5. Almost certain	H	H	E	E	E
	4. Likely	M	H	H	E	E
	3. Possible	L	M	H	E	E
	2. Unlikely	L	L	M	H	E
	1. Rare	L	L	M	H	H

Matrix Analisis Risiko menggunakan kuadran untuk memetakan kemungkinan risiko terjadi terhadap konsekuensi (atau dampak) risiko yang akan memiliki. Australia / Selandia Baru ISO 31000: 2009 Manajemen Risiko-Prinsip dan Pedoman **(AS / NZS ISO 31000: 2009, lihat http://infostore.saiglobal.com/store/Details.aspx? ProductID¼1378670)** menjelaskan Matrix Analisis Risiko, ditunjukkan pada **Tabel 3.1.**

Matrix Analisis Risiko memungkinkan Anda untuk melakukan Kualitatif Analisis Risiko (lihat Bagian "Kualitatif dan Analisis Risiko Kuantitatif") berdasarkan kemungkinan (dari "Langka" untuk "hampir pasti") dan konsekuensi (atau dampak), dari "tidak signifikan" untuk "Bencana." Skor yang dihasilkan rendah **(L)**, sedang **(M)**, tinggi **(H)**, dan ekstrim risiko **(E)**. Risiko rendah ditangani melalui proses normal, risiko moderat memerlukan manajemen pemberitahuan, risiko tinggi memerlukan pemberitahuan manajemen senior, dan risiko ekstrim memerlukan tindakan segera termasuk rencana mitigasi rinci **(dan pemberitahuan manajemen senior).** Tujuan dari matriks adalah untuk mengidentifikasi risiko tinggi kemungkinan / high-konsekuensi **(Kuadran kanan atas Tabel 3.1)** dan mengusir mereka ke rendah kemungkinan / lowconsequence risiko **(kuadran kiri bawah Tabel 3.1).**

E. Menghitung Annualized Loss Expectancy

The Annualized Loss Expectancy (ALE) perhitungan memungkinkan Anda untuk menentukanbiaya tahunan kerugian akibat risiko. Setelah dihitung, ALE memungkinkan Anda untuk membuat keputusan untuk mengurangi risiko. Bagian ini akan menggunakan contoh resiko karena laptop tidak terenkripsi hilang atau dicuri. Asumsikan perusahaan Anda memiliki 1.000 laptop yang berisi informasi pribadi (PII). Anda adalah petugas keamanan, dan Anda khawatir tentang risiko paparan dari PII karena hilang atau dicuri laptop. Anda ingin membeli dan menyebarkan solusi enkripsi laptop. Solusinya adalah mahal, sehingga Anda perlu meyakinkan manajemen yang solusinya adalah berharga.

Nilai Aktiva

Nilai Aktiva **(AV)** adalah nilai aset Anda mencoba untuk melindungi. Dalam contoh ini, masing-masing laptop biaya $ 2500, tapi nilai riil adalah PII. Pencurian tidak terenkripsi PII telah terjadi sebelumnya dan telah menelan biaya perusahaan berkali-kali nilai laptop denda peraturan, publisitas buruk, biaya hukum, jam staf menghabiskan menyelidiki, dll Nilai Aktiva rata sebenarnya dari sebuah laptop dengan PII untuk contoh ini adalah $ 25.000 ($ 2.500 untuk perangkat keras dan $ 22.500 untuk terkena PII). Aset berwujud (seperti komputer atau bangunan) yang mudah untuk menghitung. Aset tidak berwujud yang lebih menantang. Misalnya, apa nilai loyalitas merek? Menurut Deloitte, ada tiga metode untuk menghitung nilai aset tidak berwujud, pendekatan pasar, pendekatan pendapatan, dan pendekatan biaya:

• "Pendekatan Pasar: Pendekatan ini mengasumsikan bahwa nilai wajar aset mencerminkan

harga yang sebanding aset telah dibeli dalam transaksi di bawah kondisi yang sama.

• Pendekatan Pendapatan: Pendekatan ini didasarkan pada premis bahwa nilai dari

keamanan atau aset adalah nilai sekarang dari kapasitas produktif masa depan yang merupakan aset

akan menghasilkan lebih dari sisa masa manfaatnya.

• Pendekatan Biaya: Pendekatan ini memperkirakan nilai wajar aset dengan mengacu

biaya yang akan dikeluarkan untuk menciptakan atau mengganti aset. "1

Biaya Total Kepemilikan

Total Cost of Ownership (TCO) adalah total biaya dari perlindungan yang meringankan. TCO menggabungkan biaya dimuka (sering biaya modal satu kali) ditambah biaya tahunan pemeliharaan, termasuk staf jam, biaya pemeliharaan penjual, langganan software, dll.

Biaya-biaya yang berkelanjutan biasanya dianggap biaya operasional.

Table 3.2 Summary of Risk Equations

	Formula	Description
Asset Value (AV)	AV	Value of the asset
Exposure Factor (EF)	EF	Percentage of Asset Value lost
Single Loss Expectancy (SLE)	AV × EF	Cost of one loss
Annual Rate of Occurrence (ARO)	ARO	Number of losses per year
Annualized Loss Expectancy (ALE)	SLE × ARO	Cost of losses per year

Menggunakan contoh enkripsi laptop kami, biaya dimuka perangkat lunak enkripsi laptop adalah $ 100 / laptop, atau $ 100.000 untuk 1000 laptop. Vendor biaya 10% per tahun Biaya dukungan atau $ 10,000 / tahun. Anda memperkirakan bahwa ia akan mengambil 4 jam staf per laptop untuk menginstal perangkat lunak atau 4000 jam staf. Staf yang akan melakukan pekerjaan ini membuat $ 50 / jam plus keuntungan. Termasuk manfaat, biaya staf per jam adalah $ 70 kali 4000 jam, yaitu $ 280.000. Perusahaan Anda menggunakan 3-tahun teknologi refresh siklus, sehingga Anda menghitung total Biaya Kepemilikan lebih dari 3 tahun:

• Biaya Software: $ 100,000

• dukungan vendor Tiga tahun: $ 10,0003¼ $ 30.000

• biaya staf Per Jam: $ 280,000

• Biaya Total Kepemilikan lebih dari 3 tahun: $ 410,000

• Biaya Total Kepemilikan per tahun: $ 410.000 / 3¼ $ 136.667 / tahun

Tahunan Biaya Total Kepemilikan untuk proyek enkripsi laptop adalah $ 136.667 per tahun.

Return on Investment

Return on Investment (ROI) adalah jumlah uang yang disimpan dengan menerapkan menjaga. Jika Total Biaya tahunan Kepemilikan **(TCO)** adalah kurang dari Annualized Anda Rugi Harapan **(ALE)**, Anda memiliki ROI yang positif (dan telah membuat baik Pilihan). Jika TCO lebih tinggi dari ALE Anda, Anda telah membuat pilihan yang buruk. TCO tahunan enkripsi laptop adalah $ 136.667; Rugi Harapan Annualized untuk laptop tidak terenkripsi hilang atau dicuri adalah $ 275.000. Matematika diringkas dalam **Tabel 3.3.**

Table 3.3 Annualized Loss Expectancy of Unencrypted Laptops

	Formula	Value
Asset Value (AV)	AV	$25,000
Exposure Factor (EF)	EF	100%
Single Loss Expectancy (SLE)	AV × EF	$25,000
Annual Rate of Occurrence (ARO)	ARO	11
Annualized Loss Expectancy (ALE)	SLE × ARO	$275,000

Menerapkan enkripsi laptop akan mengubah Factor Exposure. Laptop hardware bernilai $ 2500, dan terkena PII biaya tambahan $ 22.500 untuk $ 25.000 Nilai Aktiva. Jika laptop tidak terenkripsi hilang atau dicuri, Faktor Exposure adalah 100% (hardware dan semua data terkena). Enkripsi laptop meringankan PII eksposur risiko, menurunkan Factor Exposure dari 100% (laptop dan semua data) ke 10% (hanya hardware laptop). Semakin rendah Factor Exposure menurunkan Loss Expectancy Annualized dari $ 275.000 untuk $ 27.500 seperti yang ditunjukkan pada **Tabel 3.4.**

Table 3.4 Annualized Loss Expectancy of Encrypted Laptops

	Formula	Value
Asset Value (AV)	AV	$25,000
Exposure Factor (EF)	EF	10%
Single Loss Expectancy (SLE)	AV × EF	$2500
Annual Rate of Occurrence (ARO)	ARO	11
Annualized Loss Expectancy (ALE)	SLE × ARO	$27,500

Return on Investment Anda akan menghemat $ 247.500 / tahun (ALE tua, $ 275.000, dikurangi ALE baru, $ 27.500) dengan membuat investasi $ 136.667. ROI Anda adalah $

110.833 per tahun ($ 247.500 dikurangi $ 136.667). Proyek enkripsi laptop memiliki ROI yang positif dan adalah investasi yang bijaksana.

Analisis Risiko Kualitatif dan Kuantitatif

Analisis Risiko Kuantitatif dan Kualitatif dua metode untuk menganalisis risiko.

Analisis Risiko Kuantitatif menggunakan metrik keras, seperti dolar. Risiko kualitatif Analisis menggunakan nilai perkiraan sederhana. Kuantitatif lebih objektif; kualitatif lebih subjektif. Analisis Risiko Hybrid menggabungkan dua:

menggunakan kuantitatif analisis untuk risiko yang mungkin mudah dinyatakan dalam nomor keras, seperti uang, dan kualitatif untuk sisanya.

Proses Manajemen Risiko

panduan menjelaskan proses Analisis Risiko 9-langkah:

1. Sistem Karakterisasi

2. Ancaman Identifikasi

3. Kerentanan Identifikasi Analisis

4. Kontrol Penentuan

5. Kemungkinan

6. Analisa Dampak Penentuan

7. Risiko

8. Kontrol Rekomendasi

9. Hasil Dokumentasi

F. KEAMANAN INFORMASI TATA

Keamanan Informasi Pemerintahan adalah keamanan informasi di tingkat organisasi: manajemen senior, kebijakan, proses, dan staf. Itu juga merupakan prioritas organisasi disediakan oleh kepemimpinan senior, yang diperlukan untuk informasi yang berhasil program keamanan.

Kebijakan keamanan dan dokumen terkait

Dokumen seperti kebijakan dan prosedur adalah bagian yang diperlukan dari setiap sukses program keamanan informasi. Dokumen-dokumen ini harus didasarkan pada realitas: mereka tidak dokumen idealis yang duduk di rak-rak mengumpulkan debu. Mereka harus mencerminkan dunia nyata dan memberikan bimbingan pada benar (dan kadang-kadang diperlukan) cara melakukan hal-hal.

Polis

Kebijakan yang arahan manajemen tingkat tinggi. Kebijakan adalah wajib: jika Anda tidak setuju dengan kebijakan pelecehan seksual perusahaan Anda, misalnya, Anda tidak memiliki pilihan untuk tidak mengikutinya.

Prosedur

Berikut ini adalah contoh prosedur sederhana untuk membuat user baru:

1. Menerima formulir permintaan baru-pengguna dan memverifikasi kelengkapan.

2. Pastikan bahwa manajer pengguna telah menandatangani formulir.

3. Pastikan bahwa pengguna telah membaca dan setuju dengan kebijakan keamanan akun pengguna.

4. Klasifikasikan peran pengguna dengan mengikuti prosedur peran-tugas NX-103.

5. Pastikan bahwa pengguna telah memilih "kata rahasia," seperti gadis ibu mereka

nama, dan masukkan ke dalam profil akun help desk.

6. Buat account dan menetapkan peran yang tepat.

7. Menetapkan kata rahasia sebagai password awal dan mengatur "Angkatan pengguna untuk mengubah password pada login berikutnya untuk 'Benar'. "

8. E-surat dokumen Akun Baru ke pengguna dan manajer mereka.

Langkah-langkah dari prosedur ini adalah wajib. Administrator keamanan tidak memiliki

pilihan untuk melewatkan langkah 1, misalnya, membuat akun tanpa formulir.

Standar

Sebuah standar menggambarkan penggunaan khusus dari teknologi, sering diterapkan untuk perangkat keras dan software. "Semua karyawan akan menerima ACME Nexus-6 laptop dengan 4 gigabyte memori, 2,8 GHZ dual core CPU, dan 2-Terabyte disk "adalah contoh dari

perangkat keras standar. "Laptop akan menjalankan Windows 8 Enterprise, versi 64-bit" adalah Contoh dari perangkat lunak (sistem operasi) standar.

Pedoman

Pedoman adalah rekomendasi (yang diskresioner). Pedoman A bisa menjadi berguna nasihat, seperti "Untuk membuat password yang kuat, mengambil huruf pertama dari setiap kata dalam kalimat, dan campuran dalam beberapa angka dan simbol. "Aku akan melewati CISSP® yang ujian dalam 6 bulan! 'menjadi' Iwptcei6m! '. "

Baseline

Baseline adalah diskresioner: dapat diterima mengeras sistem tanpa mengikuti

benchmark tersebut, selama itu setidaknya aman seperti sistem

mengeras menggunakan tolok ukur.

Tabel 3.5 merangkum jenis dokumentasi keamanan.

Table 3.5 Summary of Security Documentation

Document	Example	Mandatory or Discretionary?
Policy	Protect the CIA of PII by hardening the operating system	Mandatory
Procedure	Step 1: Install pre-hardened OS image. Step 2: Download patches from update server. Step 3: . . .	Mandatory
Standard	Use Nexus-6 laptop hardware	Mandatory
Guideline	Patch installation may be automated via the use of an installer script	Discretionary
Baselines	Use the CISecurity Windows Hardening benchmark	Discretionary

Peran dan tanggung jawab

Peran keamanan informasi primer meliputi manajemen senior, pemilik data, kustodian, dan pengguna. Setiap memainkan peran yang berbeda dalam mengamankan aset organisasi. Pengguna adalah peran informasi utama keamanan keempat. Pengguna harus mengikuti aturan: mereka harus mematuhi kebijakan wajib prosedur, standar, dll Mereka tidak harus menulis password mereka turun atau berbagi account, misalnya. pengguna harus dibuat sadar risiko ini dan persyaratan. Anda tidak bisa menganggap mereka akan tahu apa yang harus dilakukan atau

menganggap mereka sudah melakukan hal yang benar: mereka harus diberitahu, melaluikesadaran keamanan informasi.

Personil Keamanan

Pengguna dapat menimbulkan risiko keamanan terbesar untuk sebuah organisasi. Pemeriksaan latar belakang harus dilakukan, kontraktor harus aman dikelola, dan pengguna harus terlatih dan dibuat sadar risiko keamanan, seperti yang akan kita bahas selanjutnya. Kontrol seperti Perjanjian Menyingkap (NDA) dan perjanjian kerja terkait adalah personel direkomendasikan kontrol keamanan.

Pemeriksaan latar belakang

Organisasi harus melakukan pemeriksaan latar belakang menyeluruh sebelum mempekerjakan orang. Seorang kriminal catatan cek harus dilakukan, dan semua pengalaman, pendidikan, dan sertifikasi harus diverifikasi. Berbohong atau melebih-lebihkan tentang pendidikan, sertifikasi, dan kredensial terkait adalah salah satu contoh yang paling umum dari ketidakjujuran dalam hal proses perekrutan. Lebih pemeriksaan latar belakang menyeluruh harus dilakukan untuk peran dengan tinggi hak istimewa, seperti akses ke uang atau informasi rahasia. Pemeriksaan ini dapat termasuk penyelidikan keuangan, catatan kriminal yang lebih menyeluruh memeriksa, dan wawancara dengan teman-teman, tetangga, dan saat ini dan mantan rekan kerja.

Terminasi karyawan

Pemutusan harus menghasilkan pencabutan segera semua akses karyawan. Luarakun pencabutan, pemutusan harus menjadi proses yang adil. Ada etika dan hokum alasan untuk mempekerjakan pemutusan adil, tetapi ada juga informasi tambahan Keuntungan keamanan. Musuh terburuk organisasi dapat menjadi mantan yang tidak puas karyawan, yang, bahkan tanpa akses account yang sah, tahu di mana "lemah tempat yang. "

Kesadaran keamanan dan pelatihan

Kesadaran keamanan dan pelatihan sering bingung. Kesadaran perubahan perilaku pengguna; pelatihan menyediakan keahlian. Mengingatkan pengguna untuk tidak pernah berbagi account atau menulis password mereka turun adalah contoh kesadaran. Hal ini diasumsikan bahwa beberapa pengguna melakukan hal yang salah, dan kesadaran dirancang untuk mengubah perilaku itu.

Vendor, konsultan, dan kontraktor keamanan

Personil pihak ketiga dengan akses ke data sensitif harus dilatih dan dibuat menyadari risiko, seperti karyawan. Pemeriksaan latar belakang juga mungkin diperlukan, tergantung pada tingkat akses yang diperlukan. Kebijakan keamanan informasi, prosedur, dan bimbingan lainnya harus diterapkan juga. Kebijakan tambahan mengenai kepemilikan data dan kekayaan intelektual

harus dikembangkan. Jelas aturan mendikte mana dan ketika pihak ketiga dapat mengakses atau menyimpan data harus dikembangkan.

Outsourcing dan offshoring

Keduanya dapat menurunkan total biaya kepemilikan dengan menyediakan layanan TI dengan biaya lebih rendah. Mereka juga dapat meningkatkan sumber daya teknologi informasi dan keterampilan set dan sumber daya yang tersedia untuk perusahaan (terutama perusahaan kecil), yang dapat meningkatkan kerahasiaan, integritas, dan ketersediaan data. Sebuah Analisis Risiko menyeluruh dan akurat harus dilakukan sebelum outsourcing atau data sensitif offshoring. Jika data akan berada di negara lain, youmust memastikan bahwa hukum dan peraturan yang mengatur data diikuti, bahkan di luar yurisdiksi mereka.

Pribadi

Privasi adalah perlindungan kerahasiaan informasi pribadi. banyak organisasi tuan rumah informasi pribadi pengguna mereka: PII seperti nomor jaminan sosial, informasi keuangan seperti informasi gaji dan rekening bank tahunan 56 BAB 3 Keamanan Informasi Pemerintahan diperlukan untuk deposito penggajian, dan informasi kesehatan untuk tujuan asuransi. Kerahasiaan informasi ini harus terjamin.

Hati-hati dan due diligence

Hati-hati dan due diligence sering bingung: mereka terkait, tetapi berbeda. Karena perawatan informal; due diligence berikut proses. Pikirkan due diligence sebagai langkah luar hati-hati. Mengharapkan staf Anda untuk menjaga sistem mereka ditambal berarti Anda mengharapkan mereka untuk berhati-hati karena. Memverifikasi bahwa staf Anda telah ditambal sistem mereka adalah contoh dari due diligence.

Kelalaian

Kelalaian adalah kebalikan dari perawatan karena. Ini adalah konsep hukum yang penting. Jika kamu menderita kerugian dari PII, tetapi dapat menunjukkan hati dalam melindungi PII, Anda berada di tanah secara hukum kuat, misalnya. Jika Anda tidak dapat menunjukkan hati-hati (Anda terlalu lalai), Anda berada dalam posisi hukum jauh lebih buruk.

Praktek terbaik

Keamanan informasi praktek terbaik adalah konsensus cara terbaik untuk melindungi kerahasiaan, integritas, dan ketersediaan aset. Mengikuti praktik terbaik adalah cara untuk menunjukkan hati-hati dan due diligence.

Audit dan kontrol kerangka kerja

Sejumlah kerangka kerja pengendalian yang tersedia untuk membantu Analisis Risiko audit. Beberapa, seperti PCI-DSS, yang industri tertentu. Lainnya, seperti OCTAVE, ISO 17799 /27002, dan COBIT, tertutup berikutnya, yang lebih umum.

G. Sertifikasi dan Akreditasi

Sertifikasi dapat dilakukan oleh pihak ketiga yang terpercaya seperti auditor. Sertifikasi

menyelidiki sistem, memeriksa dokumentasi, dan mungkin mengamati operasi. Mereka mengaudit sistem untuk memastikan kepatuhan. Sertifikasi ini hanya rekomendasi:

sertifikasi tidak memiliki kemampuan untuk menyetujui sistem atau lingkungan. Hanya pemilik data (accreditor) dapat melakukannya.

NIST SP 800-37 menjelaskan Sertifikasi empat langkah dan proses Akreditasi:

• fase Inisiasi

• fase sertifikasi Keamanan

• Keamanan fase akreditasi

• fase pemantauan berkelanjutan

Sistem keamanan informasi dan rencana mitigasi risiko yang diteliti selama inisiasi fase. Keamanan Systemis dinilai dan didokumentasikan selama keamanan fase sertifikasi. Keputusan untuk menerima risiko yang diwakili oleh sistem yang dibuat dan didokumentasikan selama fase akreditasi keamanan. Akhirnya, setelah terakreditasi, yang keamanan yang sedang berlangsung dari sistem diverifikasi selama fase pemantauan terus menerus.

H. IKHTISAR TUJUAN UJIAN

Pemerintahan keamanan informasi menjamin bahwa organisasi memiliki informasi yang benar struktur, kepemimpinan, dan bimbingan. Tata Kelola membantu memastikan bahwa perusahaan memiliki kontrol administrasi yang tepat untuk mengurangi risiko. Analisis Risiko (RA) membantu memastikan bahwa organisasi benar mengidentifikasi, menganalisis, dan meringankan risiko. Akurat menilai risiko dan memahami istilah-istilah seperti Annualized Loss Harapan, Total Cost of Ownership, dan Return on Investment tidak hanya akan membantu Anda dalam ujian tetapi juga membantu memajukan karir keamanan informasi Anda.

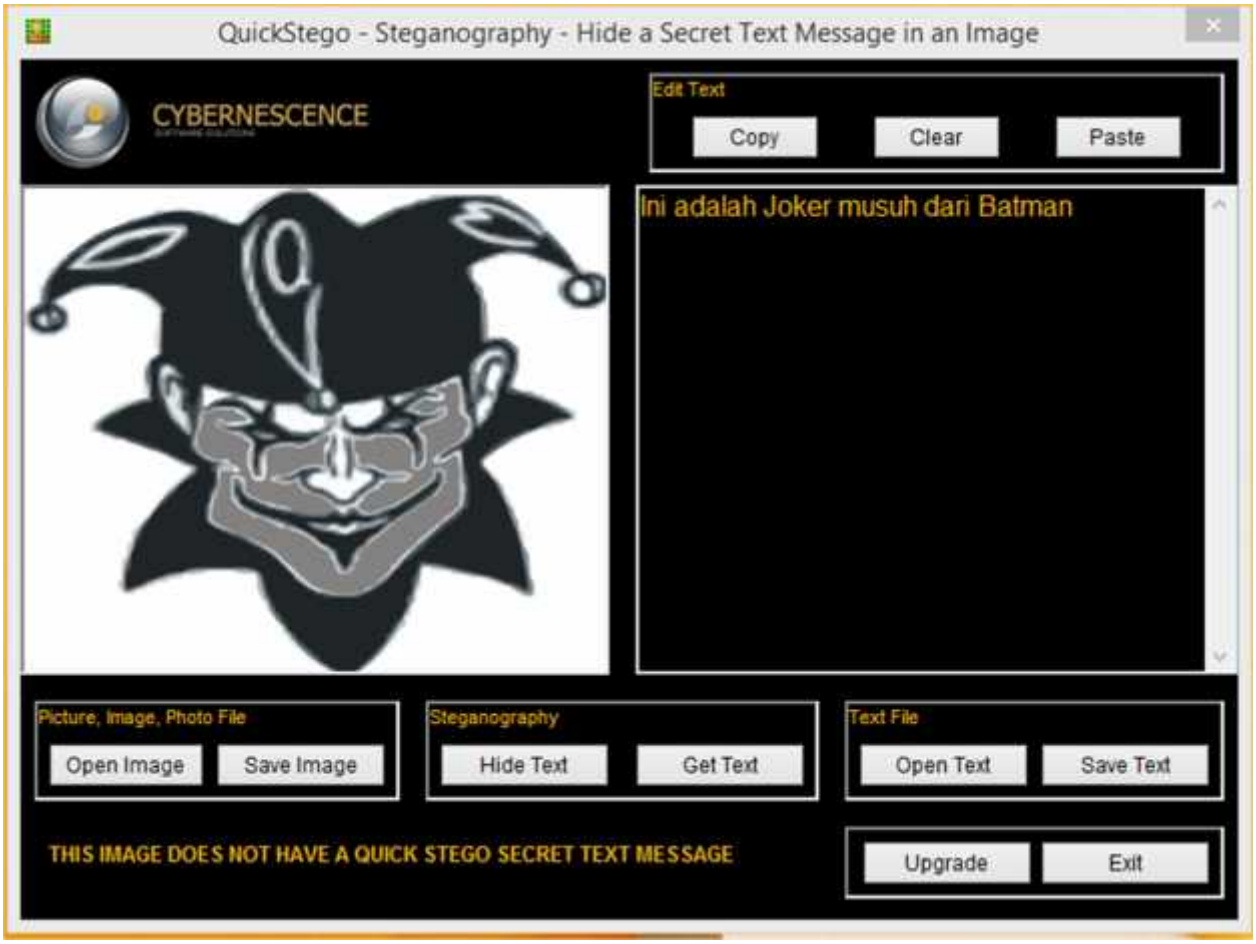
TUGAS 2

APLIKASI STEGANOGRAFI

Software QuickStego

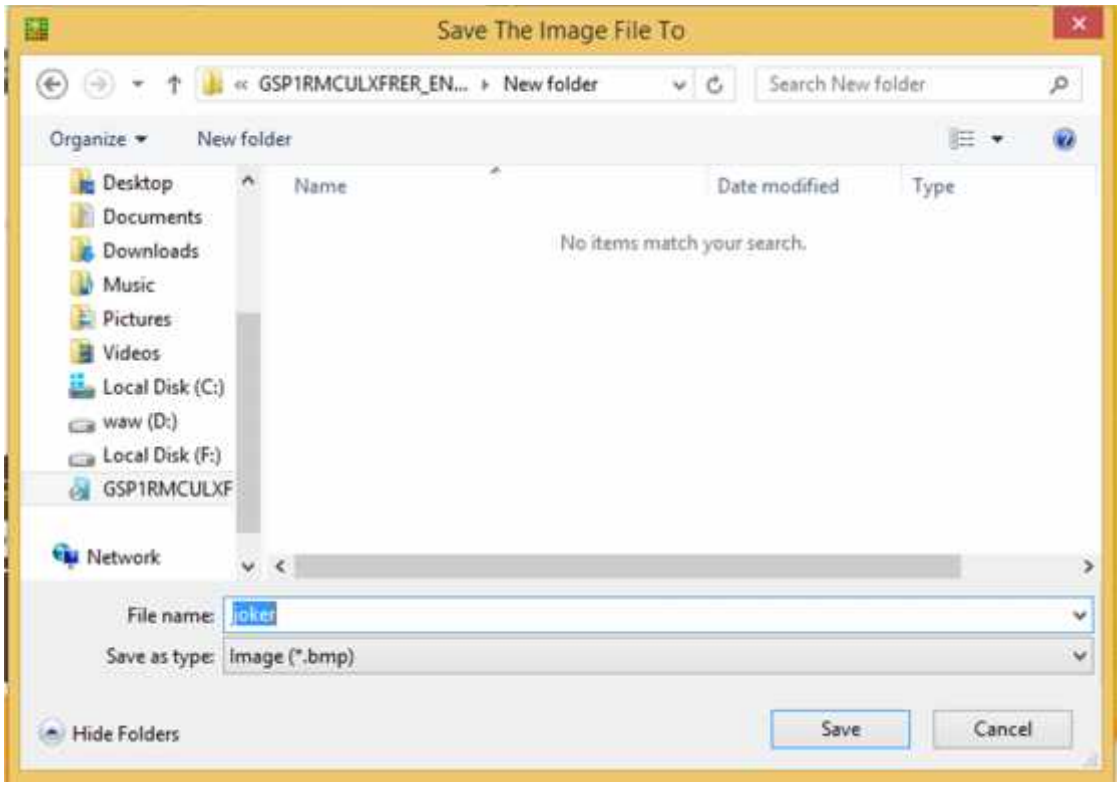
1. Buka Aplikasi QuickStego

2. Open image

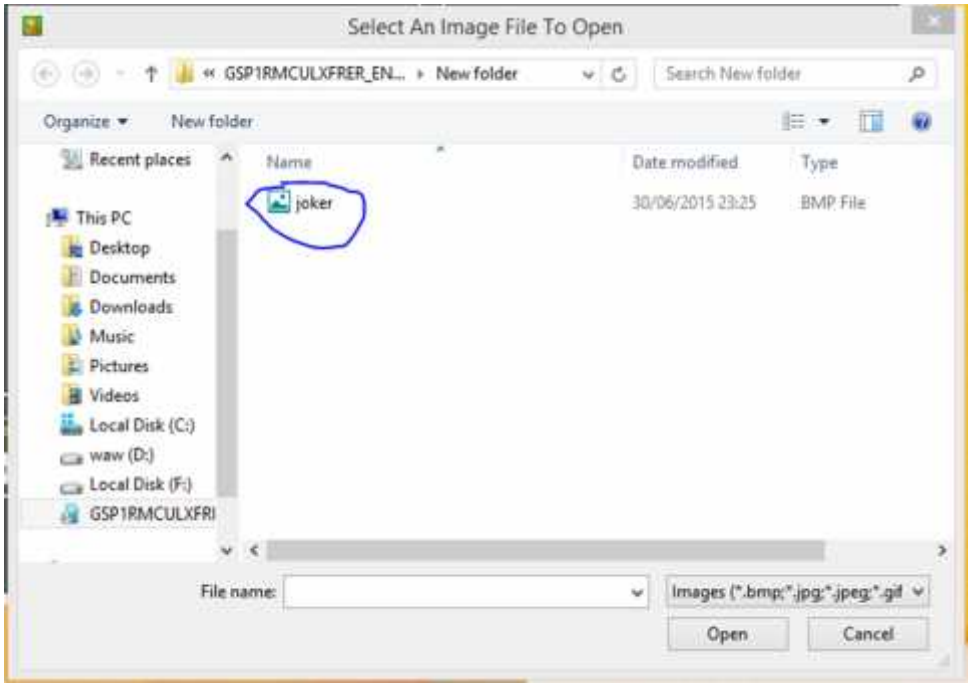


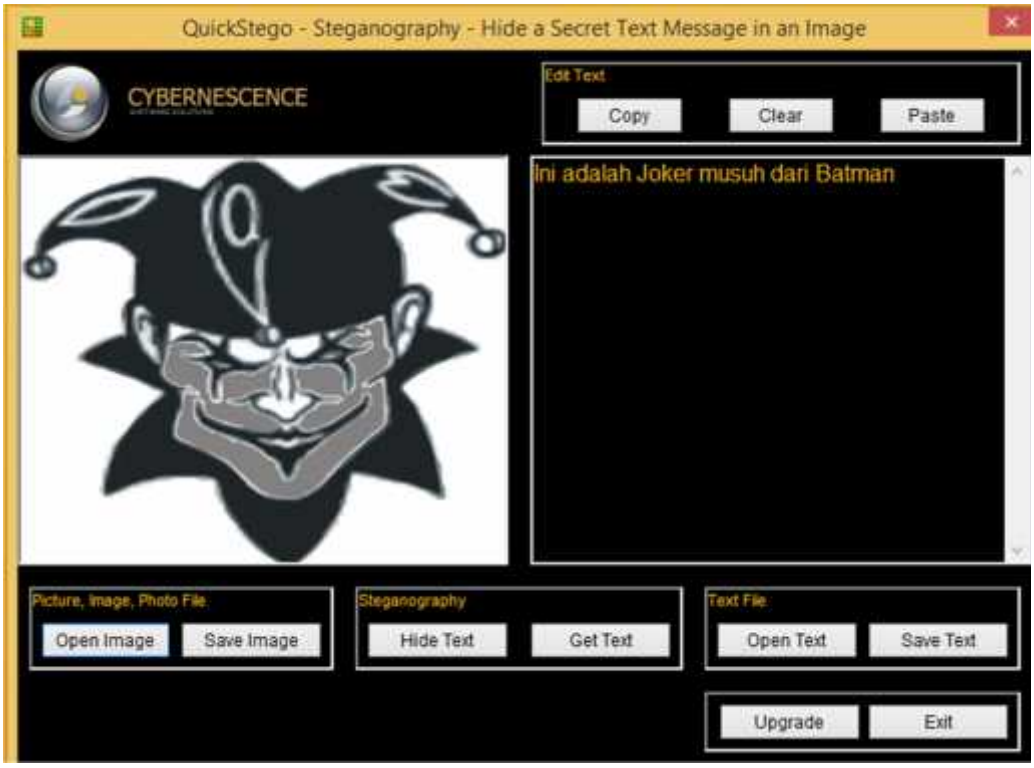
3. Kemudian ketik text yang akan di sembunyikan pada gambar yang telah kita masukan
4. Setelah text dimasukan klik “Hide Text” pada software dan Save

s



5. Setelah di save text tersebut dengan otomatis tersembunyi dalam gambar
6. Untuk melihat text yang tersimpan atau tersembunyi pada gambar kita harus membuka dengan aplikasi yang sama





7. Setelah di open text yang tersembunyi akan terlihat kembali

TERIMAKASIH