Dear Students,

You are required to complete the fist assigment for this subject.

Cheers,
Dedy

Soal (Case Study) :

Posisi anda saat ini adalah sebagai Kepala Departemen Teknologi dan Informasi yang bertanggungjawab atas sumber daya IT perusahaan dalam. Saat ini anda diminta oleh pihak senior executive baik dari divisi bisnis maupun teknologi untuk mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan. Hal ini berkaitan dengan dengan rencana penerapan kebijakan untuk

a) Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

b) Melakukan migrasi aplikasi bisnis yang kritis berikut data-data ke Cloud

c) Meng-*outsource* fungsi-fungsi IT yang penting kepada pihak ke tiga (*third parties*).

d) Migrasi teknologi desktop konvensional kepada teknologi berbasis virtual atau *Virtual Desktop Infrastructure (VDI).*

Anda diminta untuk mengidentifikasi resiko2 (*risk identification*) yang mungkin timbul dari penerapan kebijakan diatas. Selanjutnya anda diminta untuk mempersiapkan kebijakan atau menerapkan tehnologi untuk mereduksi akibat keamanan informasi yang mungkin timbul.

Silakan gunakan sumber yang ada (buku, internet dan sumber lainnya dalam memperkuat argument anda). Jangan lupa memberi kredit kepada sumber yang anda gunakan tadi !.

Hasil yang diharapkan dari tugas ini adalah artikel singkat (1 halaman) dan slide power point untuk dipresentasikan.

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*

NAMA : MOH. RENDY SEPTIYAN, S.KOM, MTA

NIM : 182420103

MATKUL : IT RISK MANAGEMENT AND DISASTER RECOVERY

KELAS : MTI2A1

Mengidentifikasi resiko yang berpotensi mengancam kelancaran bisnis perusahaan.

Hal ini berkaitan dengan rencana penerapan kebijakan yaitu

a. Mengizinkan karyawan untuk menggunakan perangkat pribadi (contohnya: laptop, tablet maupun handphone) sebagai alat kerja yang dapat mereka gunakan sebagai alat untuk menyelesaikan tugas kantornya.

Istilah ini juga disebut membawa teknologi Anda sendiri (BYOT), bawa ponsel Anda sendiri (BYOP), dan bawa komputer pribadi Anda (BYOPC) —jika diizinkan untuk diizinkan untuk menggunakan perangkat milik pribadi seseorang, daripada diminta untuk menggunakan perangkat yang disediakan secara resmi.

BYOD membuat terobosan signifikan di dunia bisnis, dengan sekitar 75% karyawan di pasar pertumbuhan tinggi seperti Brasil dan Rusia dan 44% di pasar negara maju sudah menggunakan teknologi mereka sendiri di tempat kerja. Survei telah menunjukkan bahwa bisnis tidak dapat menghentikan karyawan dari membawa perangkat pribadi ke tempat kerja. Penelitian terbagi atas manfaat. Satu survei menunjukkan sekitar 95% karyawan menyatakan mereka menggunakan setidaknya satu perangkat pribadi untuk bekerja.

Identifikasi Resiko :

1. Perusahaan harus menerapkan langkah-langkah keamanan untuk mencegah informasi berakhir di tangan yang salah
2. Keamanan BYOD sangat terkait dengan masalah simpul akhir , di mana perangkat digunakan untuk mengakses jaringan dan layanan yang sensitif dan berisiko organisasi yang menghindari risiko mengeluarkan perangkat khusus untuk penggunaan Internet (disebut Inverse-BYOD)
3. BYOD menghasilkan pelanggaran data
4. Departemen keamanan TI yang ingin memantau penggunaan perangkat pribadi harus memastikan bahwa mereka hanya memantau aktivitas yang berhubungan dengan pekerjaan atau mengakses data atau informasi perusahaan

5. BYOD juga harus mempertimbangkan bagaimana mereka akan memastikan bahwa perangkat yang terhubung ke infrastruktur jaringan organisasi untuk mengakses informasi sensitif akan dilindungi dari malware
6. Pengembang perangkat lunak dan produsen perangkat terus-menerus merilis patch keamanan untuk menangkal ancaman dari malware. Departemen TI yang mendukung organisasi dengan kebijakan BYOD harus memiliki sistem dan proses untuk menerapkan sistem perlindungan tambalan terhadap kerentanan yang diketahui dari perangkat yang dapat digunakan pengguna

Kebijakan :

1. Kebijakan BYOD dapat sangat bervariasi dari organisasi ke organisasi tergantung pada masalah, risiko, ancaman, dan budaya, sehingga berbeda dalam tingkat fleksibilitas yang diberikan kepada karyawan untuk memilih jenis perangkat. Beberapa kebijakan menentukan kisaran perangkat yang sempit yang lain memungkinkan jangkauan perangkat yang lebih luas. Terkait dengan ini, kebijakan dapat disusun untuk mencegah TI memiliki jumlah jenis perangkat yang berbeda yang tidak dapat dikelola untuk didukung. Penting juga untuk menyatakan dengan jelas bidang layanan dan dukungan mana yang merupakan tanggung jawab karyawan versus tanggung jawab perusahaan.
2. Untuk konsistensi dan kejelasan, kebijakan BYOD harus diintegrasikan dengan kebijakan keamanan keseluruhan dan kebijakan penggunaan yang dapat diterima. Untuk membantu memastikan kepatuhan dan pemahaman kebijakan, komunikasi pengguna dan proses pelatihan harus ada dan berkelanjutan.

Sumber : *https://en.wikipedia.org/wiki/Bring_your_own_device*