

TUGAS 3






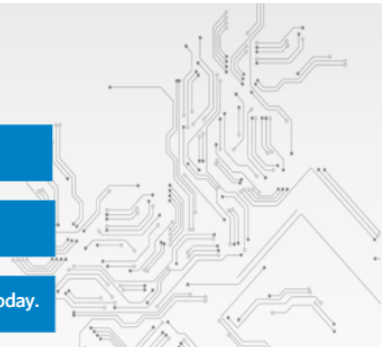
Nama	: Choirun Annas
NRP	: 3122640032
Mata Kuliah	: Keamanan Jaringan
Dosen	: Bapak Fery Astika Saputra

Resume Modul 2

Learning Objectives

By the end of this module, you will be able to:

-  Understand the impact of security incidents to organizations.
-  Understand the link between security and risk management.
-  Know some of the common security threats organizations have to deal with today.



Pada modul 2 kita akan memahami 3 aspek yaitu, memahami akibat insiden keamanan pada organisasi, Memahami hubungan antara keamanan dan resiko manajemen, Mengetahui ancaman yang umum menyerang suatu organisasi.

Why Organizations Need Security?

We learned in Module 1 that organizations need to protect their information assets.

1 Learn More **The main reason is:** Threats that exploit vulnerabilities can harm or disrupt business activities.



To deal with risk of fire, organizations place smoke detectors and fire alarms in strategic locations, do regular fire drills and buy insurance.



Similarly, organizations must identify security risks and manage them.







Suatu organisasi membutuhkan proteksi keamanan untuk menjaga bisnis dari serangan dari hacker.

Several Types of Business Impact

Before we start identifying security risks, it is good to understand the impact of security incidents to organizations.

Security incidents can impact businesses in several ways:

	Database server is down due to a Distributed Denial of Service (DDoS) attack	Business operations are disrupted due to problems related to suppliers, infrastructure malfunction, etc.
	Extra hours required to recover from mass malware infection	Cost of doing business increases
	Business is fined by local authority due to breach of customer information	Not able to deliver services based on contract. Or, not being able to comply with regulations
	Security incident causing customers to perceive that the organization is not serious about protecting customer information	Image or brand of the organization was affected

Select each icon to see examples of different types of business impacts.

Beberapa type impact bisnis dengan beberapa serangan cyber seperti :

- Database server yang terserang DDoS menyebabkan terhambatnya beberapa operasi bisnis pada organisasi.
- Tambahan waktu extra untuk melakukan recover terhadap serangan malware membuat membengkaknya biaya operasional perusahaan.
- Melanggar mengenai informasi customer membuat perusahaan rugi karena harus membayar denda.

Managing Risks

Organizations must identify and manage risks that can disrupt their activities.



Once risks have been identified and assessed in terms of their likelihood, organizations can choose to:

Mitigate

Transfer

Select each tab to learn more.



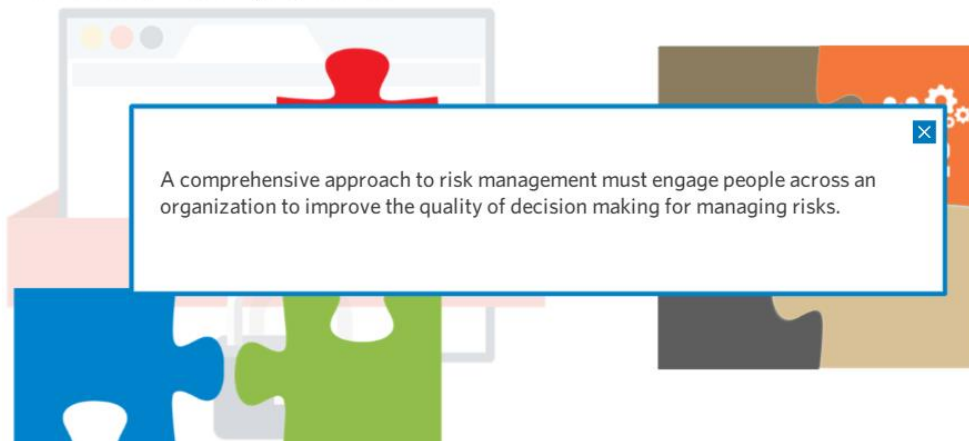
Mitigate or reduce the risk by deploying security control.

Due to the dynamic nature of the environment organizations operate in, risk assessments must be done regularly.

Untuk mengelola manajemen resiko pada suatu organisasi dengan mengurangi memperkuat dan menyebarkan control keamanan. Adapun cara lain dengan melakukan transfer beberapa data atau entitas agar aman.

Increasing Cyber Security Preparedness

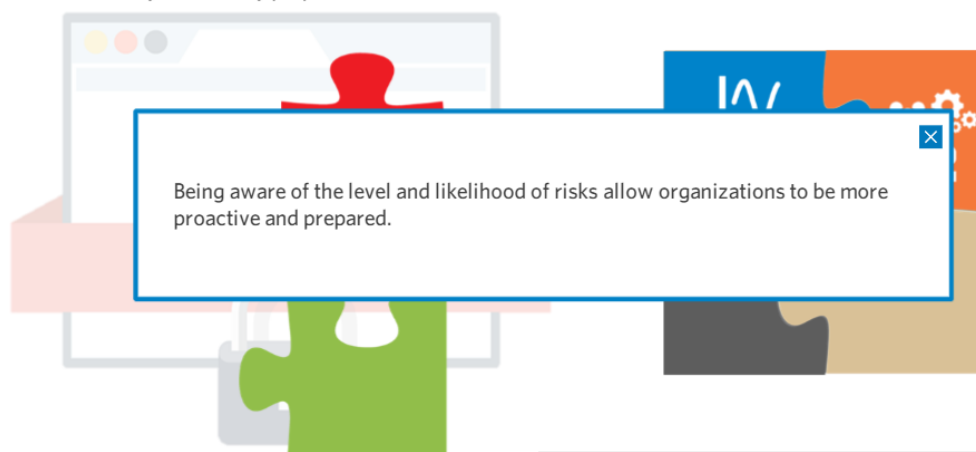
How to increase cyber security preparedness?



Untuk meningkatkan keamanan cyber dengan melatih pegawai organisasi untuk membuat keputusan yang baik untuk manajemen resiko.

Increasing Cyber Security Preparedness

How to increase cyber security preparedness?

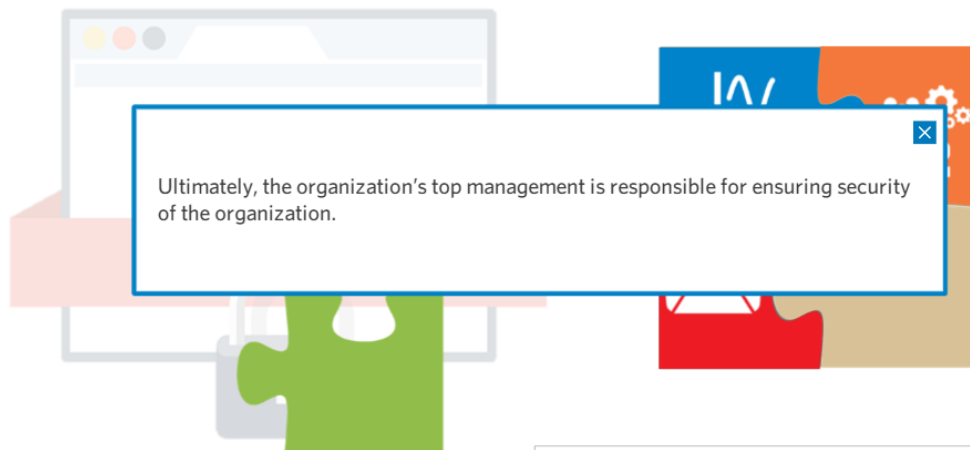


Drag and drop the puzzle pieces to its proper place to view the details.

Untuk meningkatkan keamanan dengan lebih peduli dengan level resiko yang menyerang keamanan suatu organisasi.

Increasing Cyber Security Preparedness

How to increase cyber security preparedness?



Drag and drop the puzzle pieces to its proper place to view the details.

Untuk top manajemen dari suatu organisasi dapat lebih peduli dengan control keamanan pada organisasinya.

Increasing Cyber Security Preparedness

How to increase cyber security preparedness?



Drag and drop the puzzle pieces to its proper place to view the details.

Meningkatkan keamanan suatu organisasi dengan mengadakan pelatihan pada bidang keamanan.

Common Security Threats to Organizations

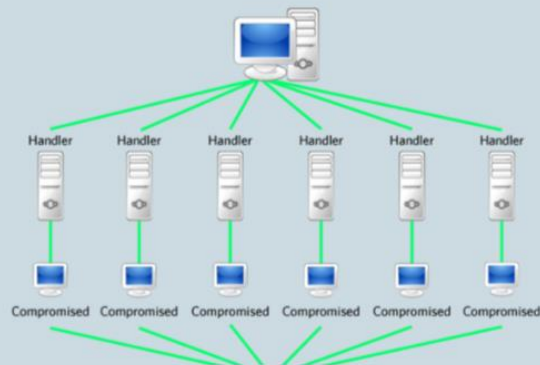
How to increase cyber security preparedness?

Denial of Service Attack

Basically, a DoS attack is carried over the network. One technique is by sending a lot of network packets, more than what the server or network equipment can process.

Organizations that have Internet-facing services such as websites, DNS and mail servers, are susceptible to this attack.

Scroll down to view the image more.



DoS attack adalah serangan cyber yang dilakukan dengan cara mengirimkan fake traffic pada suatu server atau sistem secara terus menerus, sehingga server tidak mampu mengatur semua traffic dan menyebabkan server atau sistem tersebut down.

Common Security Threats to Organizations

How to increase cyber security preparedness?

Malicious Software (Malware)

Malware stands for malicious software.

Some examples of payloads:

virus
worms
rootkits
backdoors
trojans

[Click here to view an example](#)



Malware adalah kepanjangan dari Malicious Software yang dibuat untuk untuk memasuki dan meretas sistem komputer, server atau jaringan tanpa sepengetahuan pemilik atau pengguna perangkat computer.

Common Security Threats to Organizations

How to increase cyber security preparedness?

Web Defacement

Organizations have websites to provide information and services to their customers.

Web defacement occurs when the content of the website is modified by the attackers.

It can occur due to a vulnerability in the web server software or content management system.

It can lead to unavailability of services or may affect the reputation of the organization.



Web Defacement adalah serangan keamanan siber yang bertujuan untuk merubah tampilan atau konten dari sebuah website secara ilegal.

How to Mitigate Cyber Attack Risks

It is said that in security, there is no silver bullet or one single solution that will prevent or make the security problems go away.

To deal with the risk that was mentioned earlier, we have to apply controls at various levels:



Technical Controls to Detect & Prevent

(e.g. firewalls, spam filters, intrusion detection system and antivirus software)



Education and training of our employees

especially when dealing with phishing and how to develop web application securely



Ensuring that network providers have capabilities to support us when we are under attack



Untuk mengurangi beberapa resiko serangan keamanan dengan mengontrol system dan mendeteksi serangan dengan baik, edukasi ke cyber security enginer guna mengasah hard skill, memastika koneksi provider aman dari serangan.