ÖLÇSAN
"kalitenin ölçüsü"

CYBER ATTACK
CYBER SOLUTION
CYBER INSURANCE

New Global Threat: Cyber Attack

The number of companies exposed to cyber attack or information systems breach shows that cyber risk is a real and present danger.

The strength and diversity of the cyber threat demonstrates the importance of early detection of any vulnerability.

Cyber attack is not just an IT problem, it covers the entire business and personnel.

In today's digital world, where work, education and payments are increasing, everyone connected to the business should be educated about attacks and the business should take precautions for detections.

In addition to the procedures that businesses should perform to prevent cyber attacks, the company's **cyber insurance** results in **protecting the company and data against potential problems throughout the process!**

Cyber insurance is used to protect businesses from risks associated with information technology infrastructure and operations. Risks of this nature are typically excluded from traditional commercial general liability policies, or at least not specifically identified in traditional insurance products.

New Global Threat: Cyber Attack

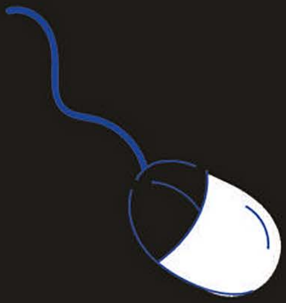
The data below, describing how serious cyber attacks can be for your business, describes the global threat's costing $6 trillion annual loss by the end of 2021!

✓**$530 million: The cost of the January 2018 Coincheck attack**, the largest cryptocurrency heist to date. (Source: Time Money)

✓Globally, cybercrime was **the second most reported crime in 2016**. (Source: PWC)

✓In proportion to the total number of crimes, cybercrime, for example, **accounts for more than 50% of all crime in the UK**. (Source: National Crime Agency)

✓**$16 billion: The Javelin Strategy & Research 2017 Fraud Report** revealed that 15.4 million U.S. consumers (up 17.5 percent) lost $16 billion to identity fraud in 2016. **This marks an increase from 2015**, when 13.1 million victims lost $15.3 billion (Source: Javelin Strategy & Research)



The Most Common Types of Cyber Attacks

Ransomware - It can take different forms, but an effective virus it infects your computer and takes control from the user. Then ransom threatens to delete all data unless paid. In 2017 WannaCry is an example of a Ransomware attack.

IoT Vulnerabilities - IoT is the "Internet of Things". These devices often have basic protections; but easier back to a network can allow the door to open.

Email/Social Engineering/Spear Phishing - This category, relates to targeted attacks against individuals. "hackers" collects the individual's personal information and attacks the person's company, data for imitation. For example, sharing like a CEO and transferring money.

IoT for DDOS attacks - This type of attack It targets and hijacks vulnerabilities in IoT devices such as security cameras. When a device is infected, it spreads the malware to other vulnerable devices, expanding its reach.

Malware - Malware is a general term covering offensive and/or unauthorized forms of software, including computer viruses, worms, Trojans, ransomware, spyware.

Phishing - It is a fraud practice through emails thought to be sent from reputable companies to obtain personal data of individuals such as credit card numbers.

The Most Common Types of Cyber Attacks

Web-Based Attacks - From buffer overflows to SQL attacks Hackers have a variety of techniques to attack Web applications.

Spam - Advertising, phishing, spreading malware, etc. for purposes, they are irrelevant or unwanted messages that are usually sent to a large number of users over the Internet.

Service Interruption - In computing, a service interruption attack is when the perpetrator interrupts a machine/network resource temporarily or indefinitely with the internet-connected host.

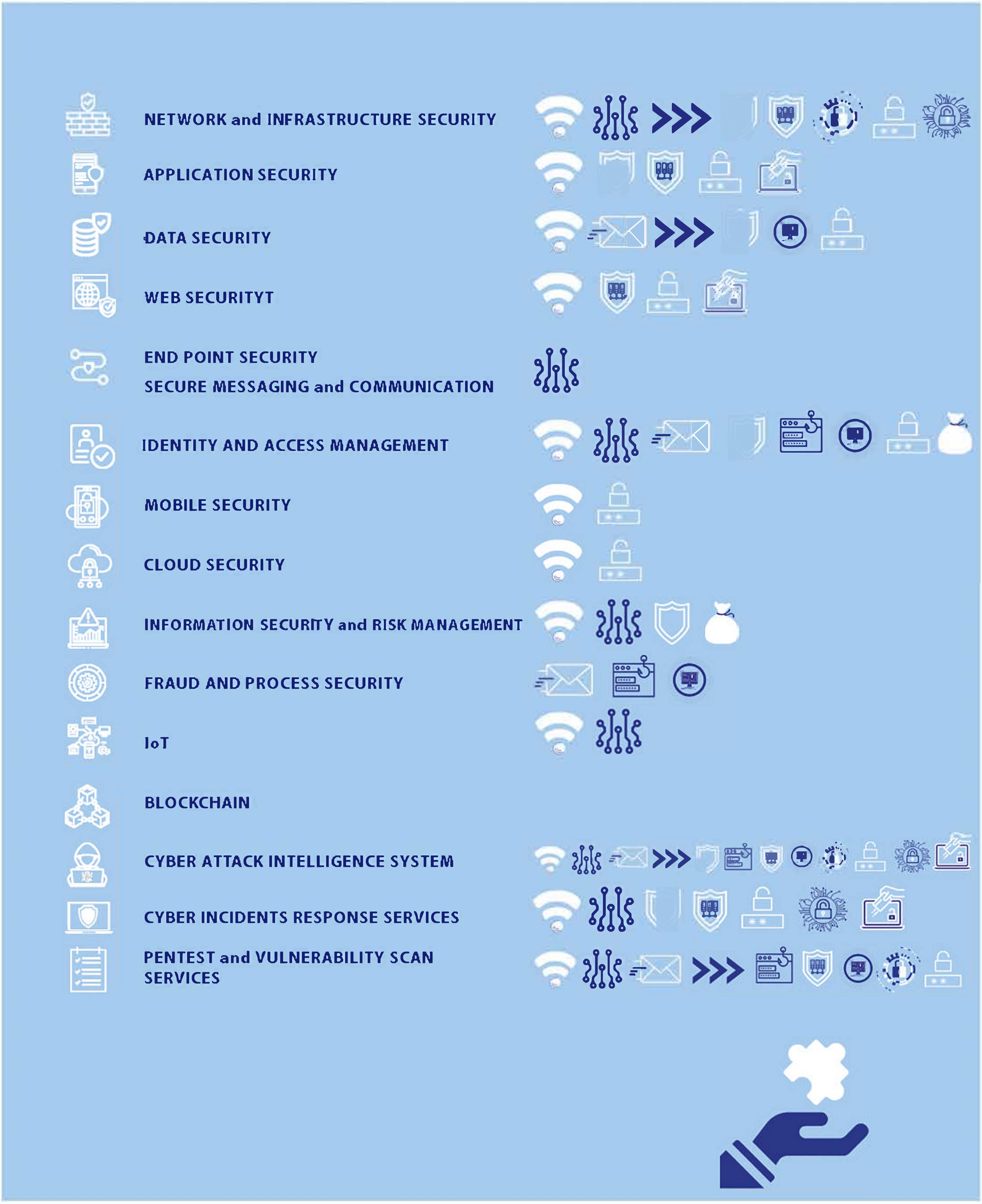
Intruder Threat - Hacker obtaining user passwords and by logging into the system. It is usually caused by easily guessed passwords or a malware **infection of the system.**

Botnet's- A network of private computers infected with malware and controlled as a group without their owners' knowledge.

Exploit Kits - A software kit of automated programs designed to run on web servers to identify software vulnerabilities on client machines communicating with it.

Physical Manipulation/damage/theft/loss - Physical manipulation of systems (eg computer theft or damage).

ÖLÇSAN's Cyber Security Solutions



NETWORK and INFRASTRUCTURE SECURITY

APPLICATION SECURITY

DATA SECURITY

WEB SECURITYT

END POINT SECURITY

SECURE MESSAGING and COMMUNICATION

IDENTITY AND ACCESS MANAGEMENT

MOBILE SECURITY

CLOUD SECURITY

INFORMATION SECURITY and RISK MANAGEMENT

FRAUD AND PROCESS SECURITY

IoT

BLOCKCHAIN

CYBER ATTACK INTELLIGENCE SYSTEM

CYBER INCIDENTS RESPONSE SERVICES

PENTEST and VULNERABILITY SCAN SERVICES

Cyber Insurance

Cyber Insurance Contracts and Cyber Business Risk Management Cover Summary

✓**Cyber Incident Response**
For Cyber Incidents reasonably suspected or confirmed;
– IT Forensics (juridical) Investigation costs
– Violation Notice
– Legal Consultancy
– Public relations
– Call center

✓**Emergency**
Incident Response included

✓**Cyber Blackmail**
In cases of cyber blackmail, coverage is provided for consultancy fees and reasonable costs to resolve the issue.

Coverage for ransom related expenses (in insurable cases)
– Bitcoin Payment Opportunity

✓**Data and System Recovery**
Coverage for data, loss, destruction, locking or corruption caused by the following situations:
– Malicious Action and Software
– Failure to provide Network Security
– Unauthorized Access
– Programming Errors
– Human Errors
– All or a part of the Computer System to mitigate the effects of the cyber incident. reasonable and necessary closures

Cyber Insurance

Cyber Insurance Additional Coverages

✓**Emergency Incident Response**

-Cyber Incident or Business Interruption that he reasonably suspects and confirms Utilizing the services of a third party forensic firm to determine the cause and scope of the incident and to initiate the process of stopping, reversing or eliminating the effects of the said Cyber Incident or Business Interruption Incident.

✓**Improvement Expenses**

-Represents the expenses for renewing or repairing the software or applications in the Computer System with newer upgraded and/or improved versions.

✓**Cyber crime**

-It is a direct financial loss that occurs exclusively in the theft of money or securities of the Insured due to malicious use or access to a computer system by third parties.

✓**Award Costs**

- Means a reasonable amount of money or other securities paid by the Insured Organization to a third party natural person who provides information that will enable the arrest or conviction of any person responsible for the Cyber Blackmail Incident.

✓**Telecommunications Fraud**

- It refers to the amount invoiced for unauthorized voice or data charges or unauthorized bandwidth to the Telecom System within the Coverage.