1

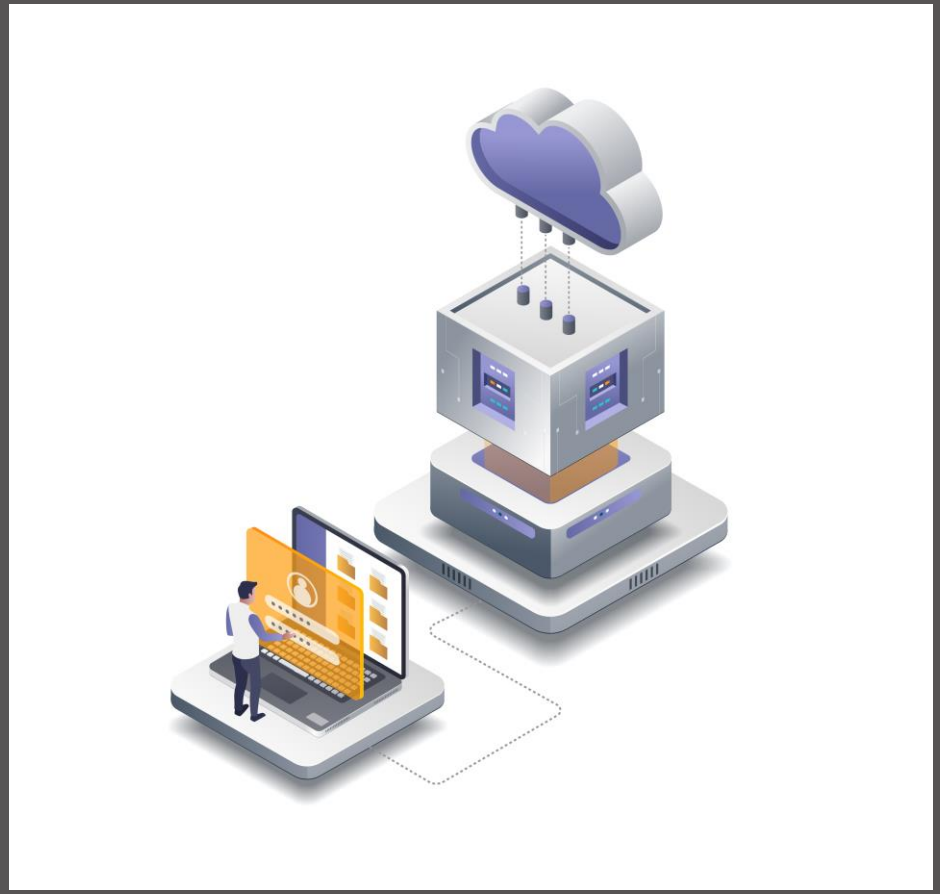
The Critical Role of Cybersecurity in Governmental Operations

The Critical Role of Cybersecurity in Governmental Operations

Cybersecurity within governmental bodies is essential for protecting the following:

1. *Sensitive information*: Governmental bodies manage a wealth of sensitive and confidential information, including personal data of citizens, classified intelligence, financial records.

2. *Ensuring national security*: Cyber threats pose significant risks to national security. Nation-states, terrorist groups and other malicious actors may target government systems to steal sensitive information.

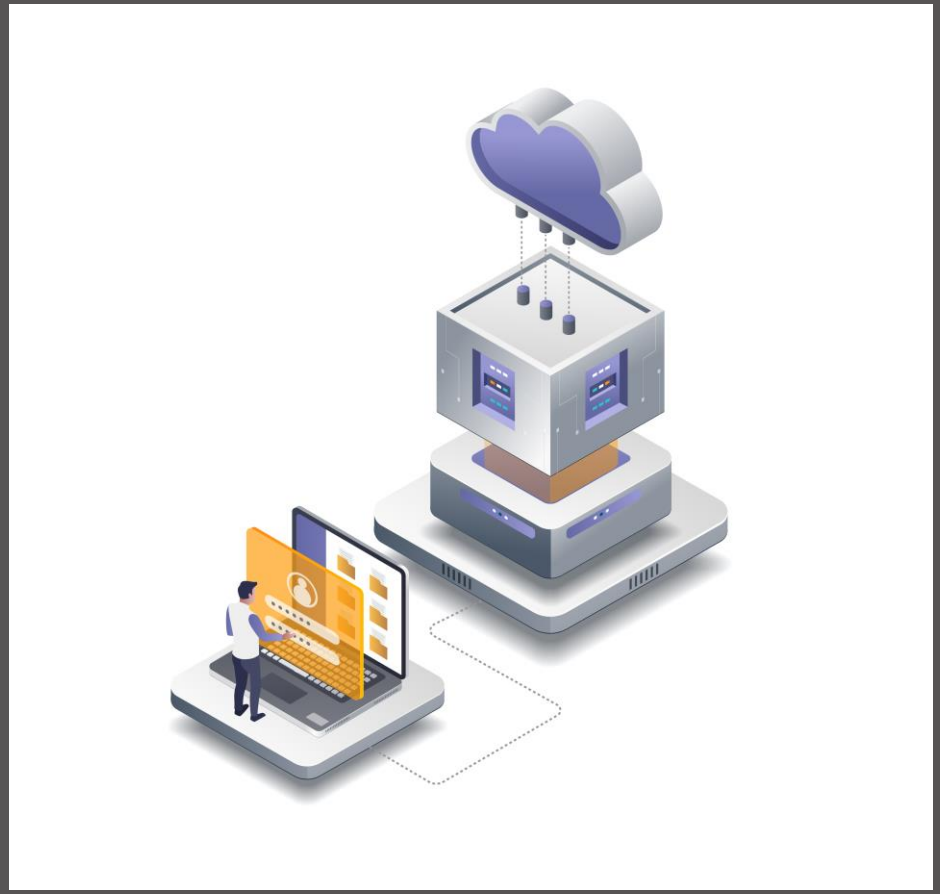


The Critical Role of Cybersecurity in Governmental Operations

Cybersecurity within governmental bodies is essential for protecting the following:

3. *Maintaining public trust*: Citizens expect their government to safeguard their personal information and ensure the reliability of public services.

4. *Ensuring operational continuity*: Cyber attacks on government ICT can disrupt essential services, causing outages, data loss, and paralysis.



The Critical Role of Cybersecurity in Governmental Operations

5. *Complying with legal requirements:* Governments must comply with laws and regulations on information protection and cybersecurity to avoid legal penalties and uphold the rule of law.

6. *Defending against cyber espionage*: Governments face cyber espionage threats aimed at stealing intelligence and intellectual property. Strong cybersecurity measures are crucial to protect sensitive information and maintain strategic advantage.

The Critical Role of Cybersecurity in Governmental Operations

7. *Safeguarding interconnected critical infrastructure*: Interconnected with sectors like healthcare, energy, and finance, government cybersecurity breaches can impact critical infrastructures, highlighting the need for robust cybersecurity measures.

2

Government Institutions facing Cybersecurity Threats

Government Institutions facing Cybersecurity Threats

Cybersecurity threats to governments can severely impact national security, public trust, and operational functionality. Key dangers include varied and significant cyber risks.:

- *Nation-State Attacks:* Foreign governments may use cyber espionage or cyber warfare to steal classified information, disrupt infrastructure, or undermine trust, often through sophisticated and well-funded attacks.

Government Institutions facing Cybersecurity Threats

- *Data Breaches:* Unauthorized access to government databases can expose personal information, classified documents, and confidential data, leading to identity theft, blackmail, and other malicious activities.

- *Ransomware:* Cybercriminals can infiltrate government systems, encrypt critical data, and demand ransoms, paralyzing operations and causing significant financial losses.

Government Institutions facing Cybersecurity Threats

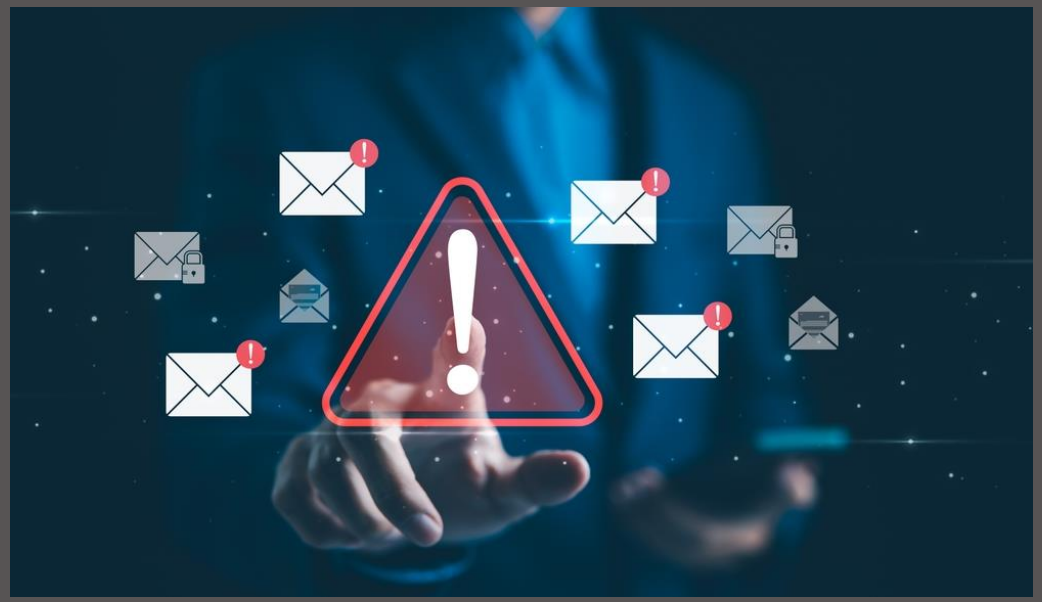
- *Phishing and Social Engineering:* Phishing emails and social engineering tactics target government employees to steal login credentials and sensitive information, potentially leading to larger security breaches.

- *Insider Threats:* Disgruntled employees or contractors can intentionally leak data or sabotage systems, making insider threats difficult to detect and mitigate.

Government Institutions facing Cybersecurity Threats

- *Denial-of-Service (DoS) Attacks:* Attackers can flood government websites with traffic, making them inaccessible and disrupting essential services and communication with the public.

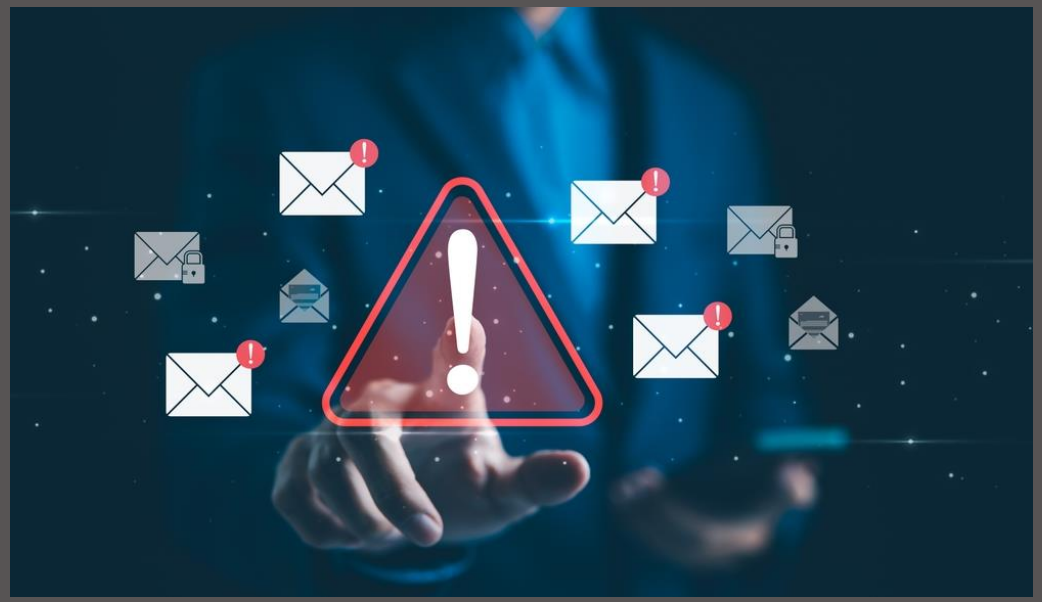
- *Supply Chain Attacks:* Compromising third-party vendors' systems can give attackers a backdoor into government networks, as agencies often rely on these vendors for software, hardware, and services.



Government Institutions facing Cybersecurity Threats

- *Malware and Viruses:* Malware can infiltrate government systems, causing data corruption, unauthorized access, and malfunctions, often spreading through email attachments, downloads, or infected websites.

- *Critical Infrastructure Vulnerabilities:* Cyber attacks on interconnected government systems and critical infrastructure sectors like energy, transportation, and healthcare can have widespread and catastrophic effects.



Government Institutions facing Cybersecurity Threats

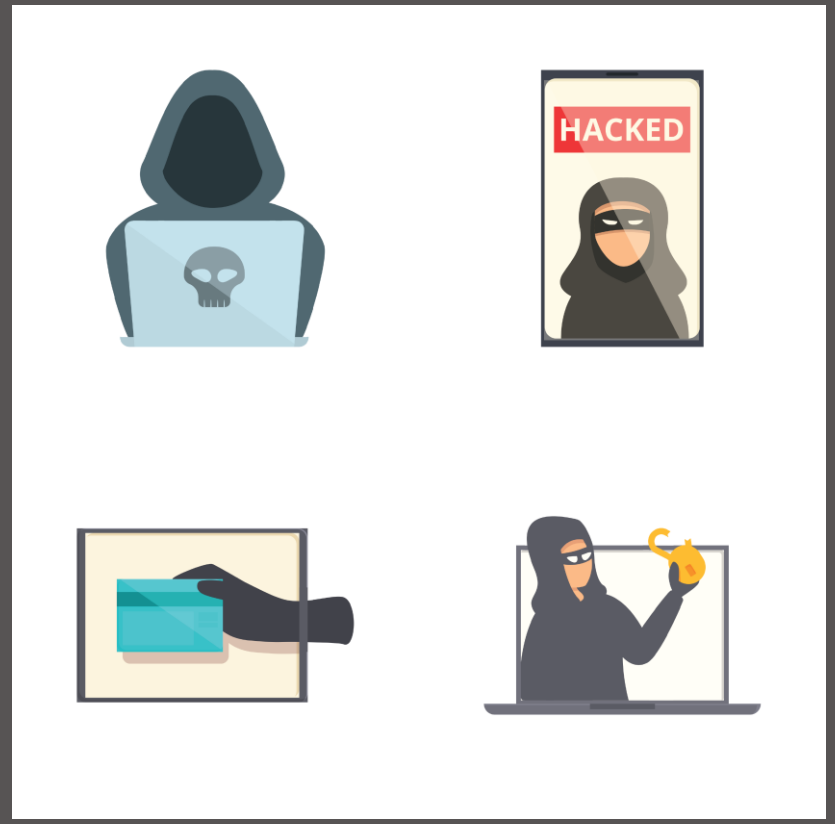
- *Zero-Day Exploits:* Attackers can exploit zero-day vulnerabilities in software or hardware, which are particularly dangerous due to the lack of immediate defenses.

- *Advanced Persistent Threats (APTs):* APTs, often conducted by nation-states, are prolonged and targeted cyber attacks aimed at stealing information or compromising systems. They are highly sophisticated and difficult to detect.

Government Institutions facing Cybersecurity Threats

- *IoT and Smart Devices:* The increasing use of IoT devices in government operations introduces new vulnerabilities, as these devices often lack robust security measures, making them attractive targets for attackers.

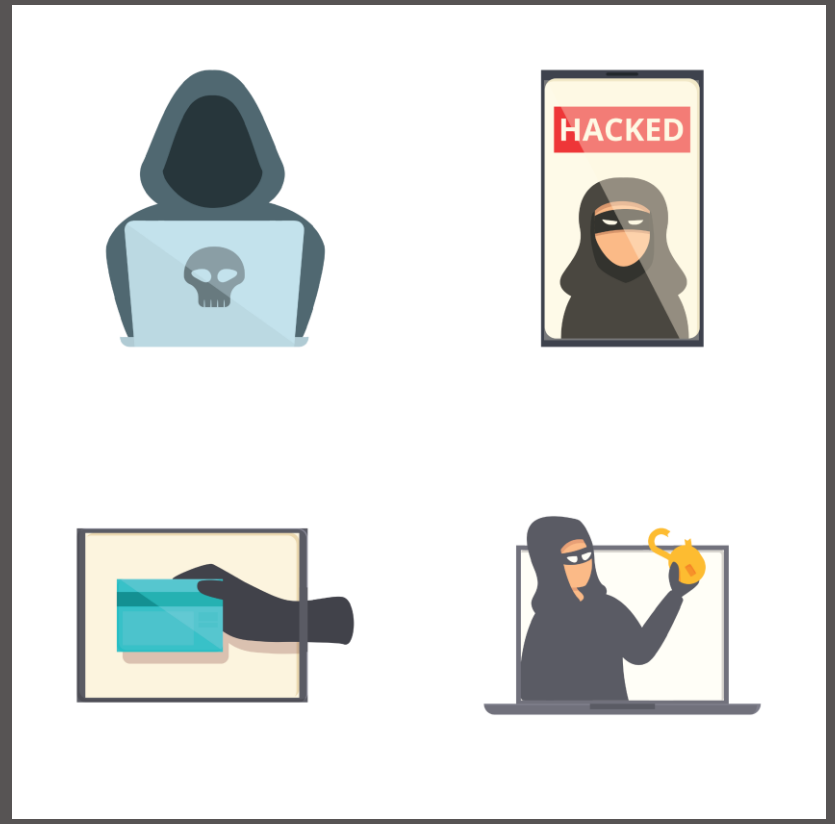
- *Lack of Cybersecurity Awareness:* Insufficient cybersecurity training and awareness among government employees heightens the risk of successful attacks, as human error is a significant factor in many security breaches.



Government Institutions facing Cybersecurity Threats

- *Cloud Security Risks:* As government agencies increasingly adopt cloud services, they must manage new security challenges related to data privacy, access control, and compliance with regulations.

- *Legacy Systems:* Many government agencies rely on outdated technology and legacy systems that may lack modern security features. These systems can be more vulnerable to attacks and harder to secure.



Government Institutions facing Cybersecurity Threats

Addressing cybersecurity dangers requires a comprehensive approach, including robust security policies, regular employee training, investment in modern security technologies, and collaboration with other agencies and private sector partners.

Effective incident response and recovery plans are also essential to minimize the impact of any security breaches that do occur.

3

Government Cybersecurity Incident Case Studies

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union
ncc.cy

July 2024:

1. South Korea's military is investigating the leak of highly sensitive information on Seoul's espionage activities and issued an arrest warrant for a suspect. The information included personal data on Seoul's non-official agents conducting undercover espionage overseas. The information was transferred to the suspect's personal laptop before being leaked. Lawmakers said the leak was first discovered in June and was not the result of a hack.

2. 2. A faulty software update for Microsoft Windows issues by cybersecurity firm CrowdStrike caused a global IT outage that disrupted airline and hospital operations. It affected approximately 8.5 million machines and cost Fortune 500 companies $5.4 billion, according to reports.

July 2024:

3. Germany accused China of directing a “serious” cyberattack against Germany’s Federal Office for Cartography and Geodesy (BKG), which conducts precision mapping of the entire country, in 2021. The findings come at the end of a three-year investigation into the incident and as Germany plans a rip-and-replace project for Chinese telecommunications infrastructure in Germany over security concerns.

July 2024:

4. Australia, the United States, Canada, the United Kingdom, Germany, Japan, South Korea, and New Zealand issued a warning about malicious Chinese state-sponsored cyber activity in their networks. It marked the first time South Korea and Japan joined with Australia to attribute malicious cyber actions to China, and the first time Australia led a cyber attribution effort against China.

June 2024:

5. Japan's space agency has suffered a series of cyberattacks since last year, according to the Japanese government. Japan's Chief Cabinet Secretary claimed the targeted networks did not contain sensitive rocket or satellite information, and that the attackers were "from outside of Japan."

6. Hackers deployed ransomware in Indonesia's national data center which briefly disrupted a variety of immigration services, including immigration document management services at airports, and deleted information that was not backed up. The attack prompted Indonesia's Director General of Informatics Applications at the Communications and Informatics Ministry to resign and initiated and a nation-wide audit of Indonesia's national data centers.

4

Government Cybersecurity Incident Case Studies Targets

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union
ncc.cy

Government Cybersecurity Incident Case Studies Targets

Typical Targeted Vulnerabilities of Government Agencies:

- **Critical Infrastructure –** They look for long-term access to gather intelligence and develop means to disable critical infrastructure and industries. Utilities such as Power and Telco companies also have vast amounts of personally identifiable information.

- **Intellectual Property** – They look to steal intellectual property that is expensive to develop in fields like high technology, medicine, defense and agriculture.

Government Cybersecurity Incident Case Studies Targets

Typical Targeted Vulnerabilities of Government Agencies:

- **Research Data** – They look to acquire such data to accelerate their own development of solutions in a variety of fields including military and bio sciences. These could have an espionage or profit motive.

- **Personal Data** – State sponsored hackers look to exploit personal data of key high – ranking officials and decision makers. This Personally Identifiable Information (PII) could be used as leverage to advance their own agenda.

5

Government Cybersecurity Best Practices

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS

COMMISSIONER OF COMMUNICATIONS Digital Security Authority

Co-funded by the European Union

ncc.cy

Social Engineering involves manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker. One of the most common forms of social engineering, is through phishing emails.

- *Align account privileges with responsibilities.*

Ensure your staff has the lowest level of privileges they require to perform their job. This can reduce the impact of successful phishing attacks.

- *Define response plan to social engineering attacks.*

Change passwords and scan for malware as soon as you suspect a phishing attack may have been successful.

Social Engineering involves manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker. One of the most common forms of social engineering, is through phishing emails.

- *Check for obvious signs of phishing and prepare for non-obvious ones*.

As a rule of thumb: If you didn't expect it – don't click on it! unless you've confirmed its legitimacy using alternative means than those provided in the email.

- *Mind your social media presence.*

Never use your business accounts to register on Social Networks or create accounts for Consumers' (free) solutions. Always be mindful of what you do online. Everything you post can and will be used against you (by attackers).

Human nature influences our emotions and how they can get the better of us.
By design, our emotions and feelings are triggered prior to our rational though. Social engineers take advantage of those triggers.

- *Curiosity*

Social engineers often exploit the human curiosity in order to compromise their target. (e.g. Dropping an infected USB in a corridor)

- *Urgency*

They also sometimes use tight deadlines to distract you from the rest of the story (e.g. Respond ASAP or your account will be deleted)

Human nature influences our emotions and how they can get the better of us.
By design, our emotions and feelings are triggered prior to our rational though. Social engineers take advantage of those triggers.

- *Authority*

Or they pretend to be a senior executive, trusted colleague, or trusted company and ask you to do something for them

- *Mimicry*

Sometimes, attackers go as far as learning your daily habits, interests and business cycles (inferred from e.g. your social media) to craft highly targeted attacks that seem absolutely legitimate.

6

Contacts of Interest in case of Cyber Incident

Contacts of Interest in case of Cyber Incident

Governmental entities in case of Cybersecurity incident must inform the authorities in charge. The authorities contact list includes the following:

- **Data Protection Commissioner**
  Tel: +357 22818456 Email: commissioner@dataprotection.gov.cy
- **CY Police Electronic Crime Division**
  Tel: +357 22808200 Email: cybercrime@police.gov.cy
- **Cyprus CSIRT**
  Tel: +357 22693094 Email: info@csirt.cy
- **Cyprus Digital Security Authority**
  Tel: +357 22693000 Email: contact@dsa.ee.cy

Thank You

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union
ncc.cy