CYBERSECURITY FOR GOVERNMENT FINANCIAL MANAGERS: SAFEGUARDING PUBLIC FUNDS IN THE DIGITAL AGE

ATTY. ABRAM M. GERONAGA, LPT
Assistant Chief
Fraud and Financial Crimes Division
NBI Manila

The government must implement cybersecurity measures not only to protect its infrastructure, but to ensure the continuous delivery of services to the people.

TOPIC GUIDE

Introduction

Cybersecurity Fundamentals for Financial Managers

Cyber Risk Factors in Public Financial Operations

Strengthening Government Cybersecurity: Prevention and Incident Mitigation

Significant Cybersecurity Laws

Key Takeaways

INTRODUCTION

GOVERNMENT FINANCIAL MANAGERS SHOULD:

Protect Public Funds

Ensure Compliance with Financial Regulations

Uphold Transparency and Accountability

INTRODUCTION

CHALLENGES OF RAPID DIGITAL TRANSFORMATION FOR GOVERNMENT FINANCIAL MANAGERS

- Legal Obligation for Digital Due Diligence
  Managers must ensure that financial systems adhere to relevant laws and policies on cybersecurity, data protection, and digital risk management.

- Expanded Scope of Accountability
  Financial oversight now includes data protection, cybersecurity integration, and digital risk management.

- Third-Party Risk Exposure
  Increased use of vendors and cloud services demands contracts with enforceable data security clauses.

- Compliance Burden
  Agencies must meet elevated standards of care in digital operations to avoid liabilities or legal violations.

- Cross-Functional Coordination Requirement
  Financial managers must engage with IT and legal teams to assess threats, design safeguards, and implement incident response plans.

- Public Trust at Stake
  Breaches in financial systems can erode confidence in government's ability to protect public funds and sensitive information

CYBERSECURITY FUNDAMENTALS FOR FINANCIAL MANAGERS

WHAT IS CYBERSECURITY?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. - *cisa.gov*

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. - *kaspersky.com*

The organization and collection of resources, processes, and structures to preserve Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity, Privacy and Safety (CIANA-PS) in cyberspace. - *NCSP 2023-2028*

CYBERSECURITY FUNDAMENTALS FOR FINANCIAL MANAGERS

WHAT IS CYBERSECURITY?

The **organization and collection of resources, processes,** and **structures** **to preserve** **Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity, Privacy and Safety** (CIANA-PS) in cyberspace. - *NCSP 2023-2028*

CYBERSECURITY FUNDAMENTALS FOR FINANCIAL MANAGERS

Organization and Collection of Resources refers to assembling all necessary tools, personnel, and knowledge to secure digital infrastructure.

- ·**Cybersecurity Tools**: Firewalls, encryption, intrusion detection systems (IDS), antivirus, etc.
- **Personnel**: Trained cybersecurity professionals, law enforcement cyber units, IT specialists.
- **Knowledge**: Threat intelligence platforms, playbooks, incident response templates.
- **Funding**: Allocating national and agency-level budgets to build secure systems.

CYBERSECURITY FUNDAMENTALS FOR FINANCIAL MANAGERS

Cybersecurity processes refer to standardized methods for managing and protecting digital assets.

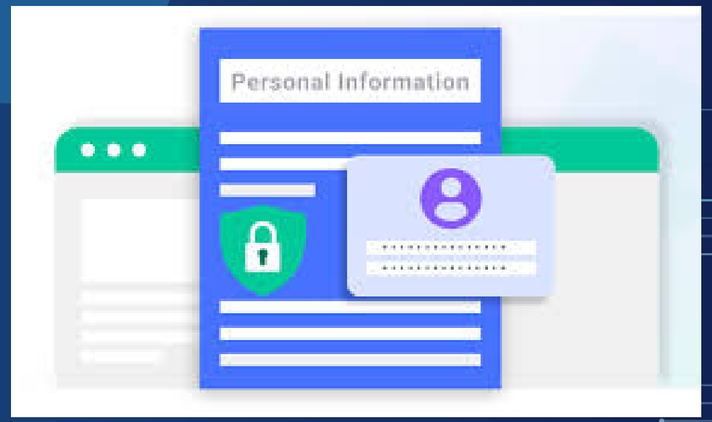
CYBERSECURITY FUNDAMENTALS FOR FINANCIAL MANAGERS

STRUCTURES INCLUDE THE ORGANIZATIONAL AND INSTITUTIONAL FRAMEWORKS THAT SUPPORT CYBERSECURITY.

CYBERSECURITY FUNDAMENTALS FOR FINANCIAL MANAGERS

Non Repudiation

Authenticity



Privacy

Safety

CYBERSECURITY FUNDAMENTALS FOR FINANCIAL MANAGERS

THERE IS A CRITICAL SKILLS GAP AMONG CYBERSECURITY PROFESSIONALS. THIS SKILLS GAP IS HIGHER FOR THE ENERGY, PUBLIC, AND BANKING AND FINANCE SECTORS.

-NCSP 2023 -2028

SKILLS GAP IN THE FINANCE SECTOR: Public Financial Management Context

Challenge	Impact
Lack of cyber workforce	Delays in detecting and responding to cyber threats
Over-reliance on third-party vendors	Exposure to **supply chain attacks** and **contractor mismanagement**.
Insufficient internal training	Increased cyber threat due to poor cyber hygiene practices
Limited budget in smaller agencies	Talent drain

Cyber Risk Factors in Public Financial Operations

Cybercriminals' Interest in Government Fiscal Operations

- Public funds and budget allocations
- Taxpayer data and payroll systems
- Procurement transactions and disbursements

Cyber Risk Factors in Public Financial Operations

Analogical Representation of Cybersecurity Components

The house represents a computer system.

- Fence & Gate = Firewalls and access controls
- Dogs = Intrusion detection or security teams
- CCTV = Monitoring and surveillance tools
- Locks = Authentication and encryption
- Environment = External digital threats

Cyber Risk Factors in Public Financial Operations

Cybersecurity Risk Elements

CYBER INCIDENTS

ATTACK SURFACE

ATTACK VECTOR

Cyber Risk Factors in Public Financial Operations

CYBER INCIDENTS

A cyber incident is an occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information it processes, stores, or transmits.

Cyber Risk Factors in Public Financial Operations

HACKING (ILLEGAL ACCESS)

Hacking refers to the unauthorized intrusion into or manipulation of a computer system, network, or digital device, typically to gain access to data, disrupt operations, or exploit vulnerabilities.

In cybersecurity and law enforcement, hacking is often associated with malicious intent, although the term can also apply to ethical or legal activities depending on context.

Cyber Risk Factors in Public Financial Operations

WHITE HAT HACKERS:
These individuals are considered ethical hackers. They use their skills to find vulnerabilities in systems with permission from the owners and help improve security. They might perform penetration testing or vulnerability assessments.

BLACK HAT HACKERS:
These hackers are known for malicious intent. They exploit vulnerabilities without authorization, often for personal gain or to cause harm. They might engage in activities like data theft or system sabotage.

GRAY HAT HACKERS:
This category falls somewhere in between white and black hats. They may discover vulnerabilities without permission and might choose to disclose them or try to sell them to the system owner for remediation. They may also use methods that are not entirely legal but may not be inherently malicious

Cyber Risk Factors in Public Financial Operations

Hacking is a cyber incedent that leads to another cyber incident. It is like a gaeway breach that can trigger a chain reaction or another attacks or damage,

- Data breach (stealing confidential data)
- Ransomware attack (locking files)
- Installation of malware or spyware
- Account takeover or identity theft
- Manipulation of system logs
- Theft or sabotage of intellectual property
- Lateral movement to other parts of the network

Cyber Risk Factors in Public Financial Operations

MALWARE INFECTION

Malware (short for malicious software) is any program or file designed to damage, disrupt, steal, or gain unauthorized access to computer systems.

Malware infection refers to the event in which malware successfully enters and compromises a computer, network, or device, often without the user's knowledge. Once inside, the malware can perform harmful actions such as stealing data, spying on users, damaging files, encrypting systems , or giving attackers remote access.

A malware infection occurs when such a program successfully installs or runs on a system without the user’s knowledge or consent

Type of Malware	Description	Effects
Viruses	Attaches to legitimate programs/files and spreads when executed.	Corrupts files, slows system, may cause crashes.
Worms	Self-replicating malware that spreads without user interaction.	Slows networks and causes major disruptions.
Trojans	Disguised as legitimate software.	Opens backdoors for hackers, steals data.
Ransomware	Encrypts files and demands ransom for decryption key.	Loss of access to data, financial loss, extortion.
Spyware	Secretly monitors user activity.	Steals sensitive data, passwords, banking info.
Adware	Displays unwanted ads, sometimes with hidden tracking.	Slows performance, invades privacy.
Rootkits	Hides malware deep in the system to avoid detection.	Provides persistent, stealthy access to system.
Keyloggers	Records every keystroke made by the user.	Captures login credentials, credit card numbers.
Botnets	Turns your device into part of a network controlled by attackers.	Used for DDoS attacks, spam, mass data theft.

Cyber Risk Factors in Public Financial Operations

DATA BREACH

A data breach is the unauthorized access, disclosure, or loss of sensitive or confidential information, including personal data like Social Security numbers or bank account information, or corporate data like customer records or intellectual property.

Essentially, it's a security incident where private information is taken or exposed without the owner's knowledge or permission.

Cyber Risk Factors in Public Financial Operations

Ransomware

Ransomware is a type of malware that restricts access to a computer system or the data it contains, typically by encrypting files or locking the system, and demands a ransom payment to restore access.

Victims are often instructed to pay the ransom, usually in cryptocurrency like Bitcoin, through an anonymous channel. Payment is not a guarantee that the attacker will restore access or data.

Cyber Risk Factors in Public Financial Operations

DEFACED WEBPAGE

Website defacement is a type of cyber attack where malicious actors alter the appearance or content of a website, often replacing the original content with their own messages or malicious code.

It's essentially an act of digital vandalism, where hackers replace a website's content with their own, often with political, religious, or simply disruptive intent

Cyber Risk Factors in Public Financial Operations

DEFACED WEBPAGE

EFFECTS OF WEBSITE DEFACEMENT

- Reputational Damage
  Damages the professional image of the organization/agency
- Financial Loss
  May lead to loss of clients or customers.
- Indicator of Security Flaws
  Indicates deeper vulnerabilities such as outdated software, weak access controls, or insecure servers

Cyber Risk Factors in Public Financial Operations

DDOS ATTACK

A Distributed Denial-of-Service (DDoS) attack is a cyberattack that floods a target with excessive traffic, making it unavailable to legitimate users.

This is achieved by using multiple sources (often compromised devices called botnets) to overwhelm the target's network or server with malicious requests.

Cyber Risk Factors in Public Financial Operations

ATTACK SURFACE

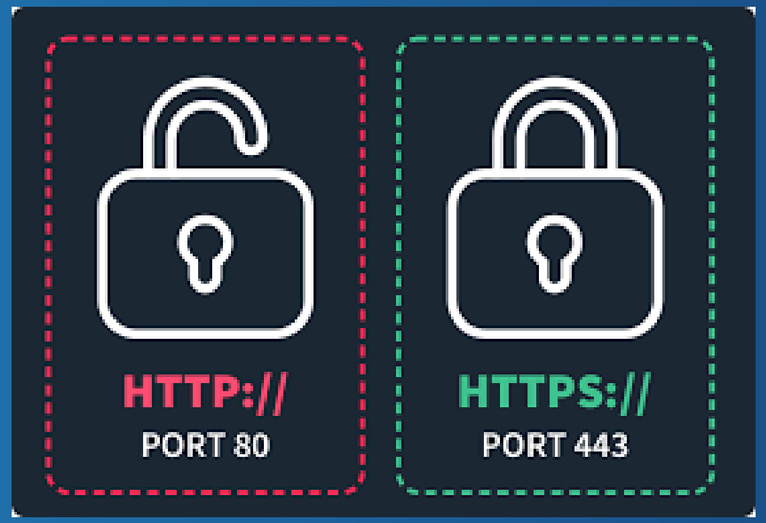
An "attack surface" in cybersecurity refers to the sum of all potential vulnerabilities and points of access that an attacker can exploit to gain unauthorized entry into a system or network. It's the entire area of an organization or system that is susceptible to hacking.

Cyber Risk Factors in Public Financial Operations

OPEN PORTS

An open port is a pathway through which a computer accepts incoming communications from other devices. Although vital for legitimate network services, an unsecured open port becomes a prime target for malicious actors.

Cyber Risk Factors in Public Financial Operations



COMMONLY USED NETWORK PORTS

Port 22 (SSH)
Securely logs you into a remote machine and encrypts all data sent.

Port 53 (DNS)
Translates domain names (e.g., example.com) into IP addresses so your browser knows where to go.

Port 80 (HTTP)
Retrieves unencrypted web pages when you type “http://...” in a browser.

Port 443 (HTTPS)
Retrieves encrypted web pages when you type “https://...”; all data is secured via TLS/SSL.

Port 25 (SMTP)
Used by mail servers to hand off outgoing email between domains.

Port 587 (SMTP Submission)
Used by mail clients to send outgoing messages with authentication (instead of using port 25).

Cyber Risk Factors in Public Financial Operations

OUTDATED SOFTWARE

KNOWN WEAKNESSES:

Outdated software typically includes security vulnerabilities that have already been identified and made public. These weaknesses are well-known within the cybersecurity community and can be easily exploited by attackers.

LACK OF PROTECTIVE UPDATES:

Software vendors regularly issue updates to correct these vulnerabilities. Failing to install these patches leaves the software exposed and susceptible to compromise.

FREQUENT TARGET OF SCANS:

Cyber attackers routinely scan networks for outdated software versions, as they can readily deploy pre-existing tools and exploits tailored to these known flaws

Cyber Risk Factors in Public Financial Operations

EMPLOYEE'S CREDENTIAL

EMPLOYEE'S CREDENTIALS (EC) AS AN ATTACK SURFACE

EC PROVIDE ACCESS

Credentials act like keys to sensitive systems, emails, files, and networks. If compromised, attackers can log in as if they were authorized users—often without raising immediate suspicion.

EC IS VULNERABLE TO THEFT

Hackers commonly use phishing, fake login pages, or malware to trick employees into revealing their usernames and passwords.

EC IS OFTEN WEAK OR REUSED

Many users rely on simple or repeated passwords across platforms, making it easier for attackers to guess or breach them.

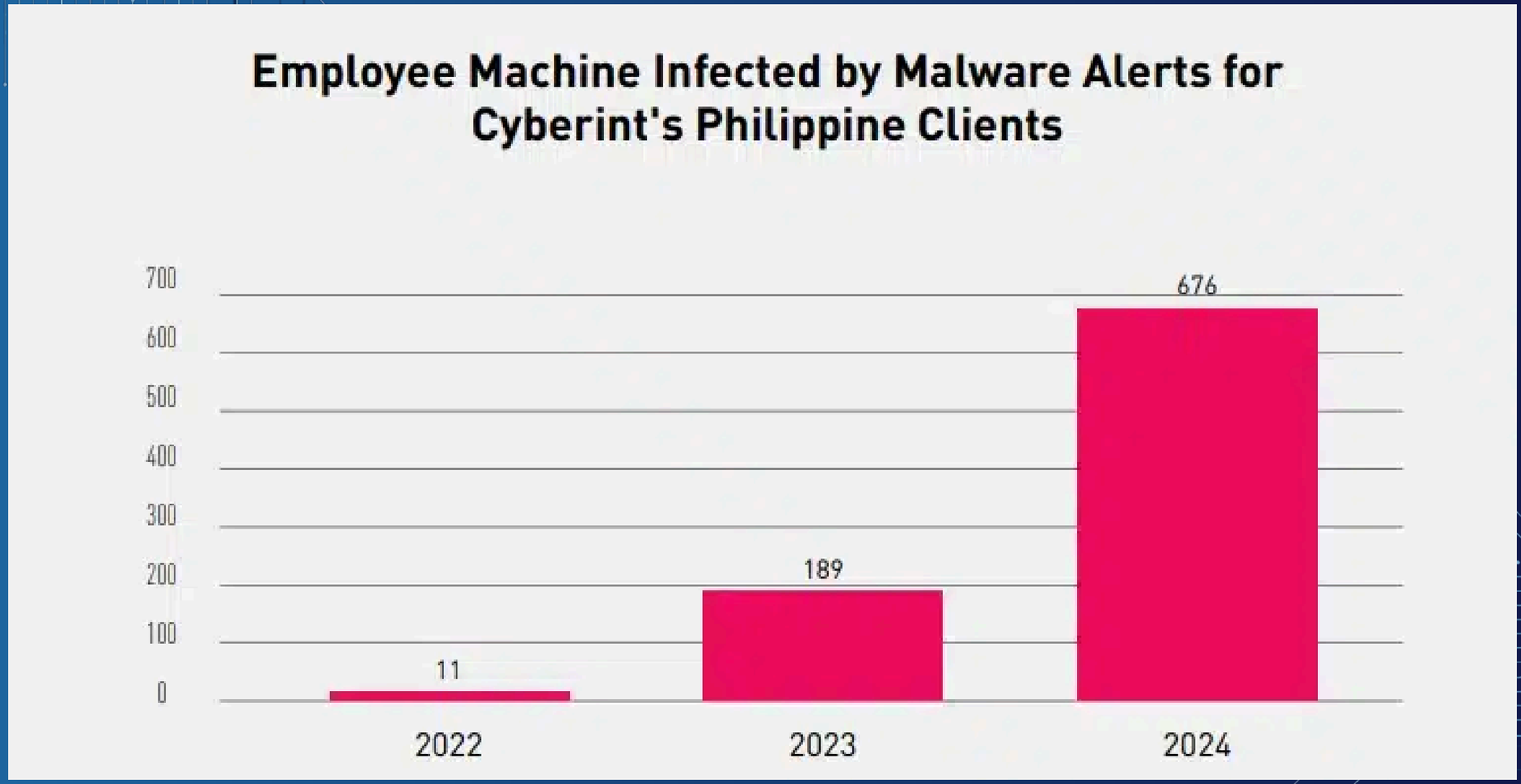
EC CAN LEAD TO FULL SYSTEM CONTROL

If the stolen credentials belong to someone with administrative privileges, attackers can gain unrestricted access to systems.

EC IS HARD TO DETECT

When valid credentials are used, malicious activity can blend in with normal operations, making it harder for security systems to identify the intrusion.

Cyber Risk Factors in Public Financial Operations



Cyber Risk Factors in Public Financial Operations

OVERSHARING IN SOCIAL MEDIA

Oversharing on social media can expose personal details like **names, birthdays, jobs, routines, or ID photos**, which attackers can use to guess passwords, send targeted phishing emails, or impersonate users.

This information helps hackers identify valuable targets, map company structures, and carry out social engineering by posing as trusted individuals to extract more sensitive data.

Cyber Risk Factors in Public Financial Operations

SOFTWARE VULNERABILITY

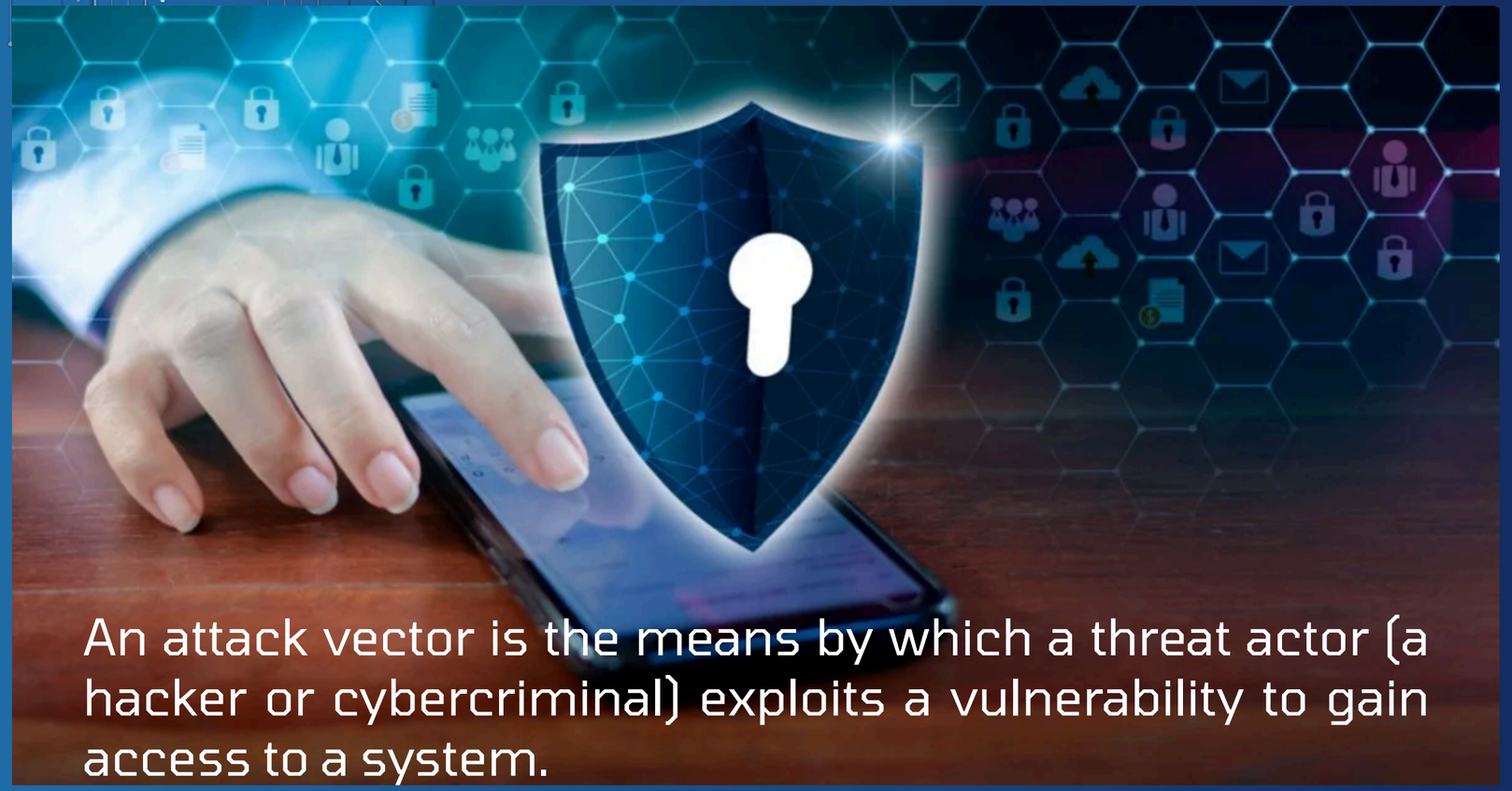
WHAT ARE SOFTWARE VULNERABILITIES?

A software vulnerability is a flaw or weakness in a computer program that can be exploited by cyber attackers to gain unauthorized access, escalate privileges, or execute malicious actions.

These flaws may be due to:

- Poor coding practices
- Lack of regular updates or patches
- Misconfigurations
- Use of outdated systems or legacy software

Cyber Risk Factors in Public Financial Operations



An attack vector is the means by which a threat actor (a hacker or cybercriminal) exploits a vulnerability to gain access to a system.

ATTACK VECTOR

Cyber Risk Factors in Public Financial Operations

PHISING

Phishing is a form of social engineering where attackers deceive userstypically via email into revealing sensitive information (like usernames, passwords, or bank details) or performing risky actions (like clicking malicious links or downloading malware)

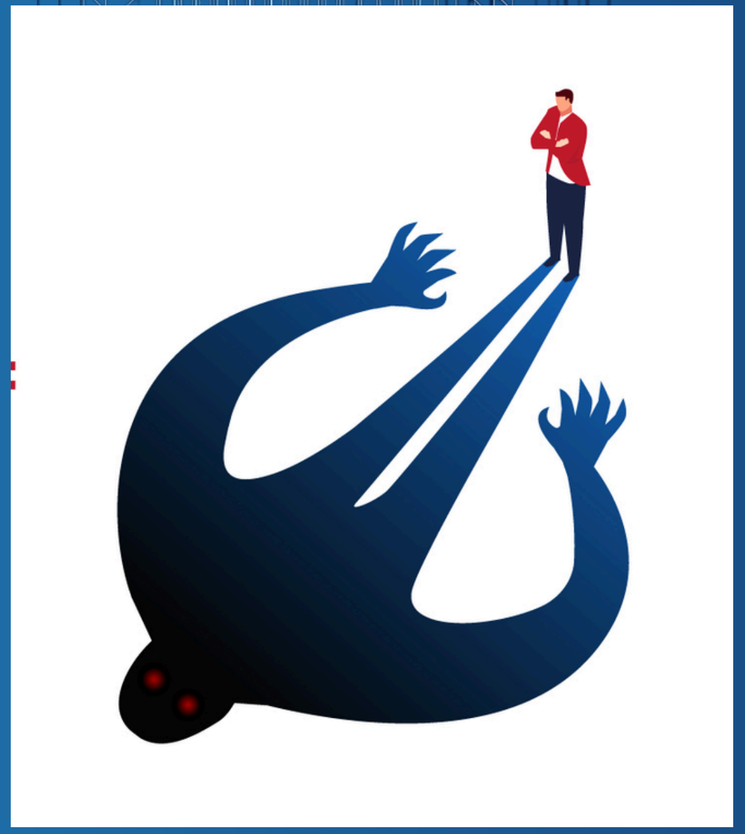
Victims are deceived to disclose, click, and download.

Cyber Risk Factors in Public Financial Operations

Area Targetted	Why it matters
Emails and other mode of electronic communication	Financial instructions are often communicated via email, making them vulnerable to impersonation or manipulation.
Procurement and payments	Attackers may send fake invoices or payment requests
Payroll and tax systems	Phishing can lead to unauthorized access to databases containing sensitive taxpayer and employee information using malware and malicious links
Login credentials	Compromised credentials can allow attackers to alter financial records or authorize illegitimate transactions

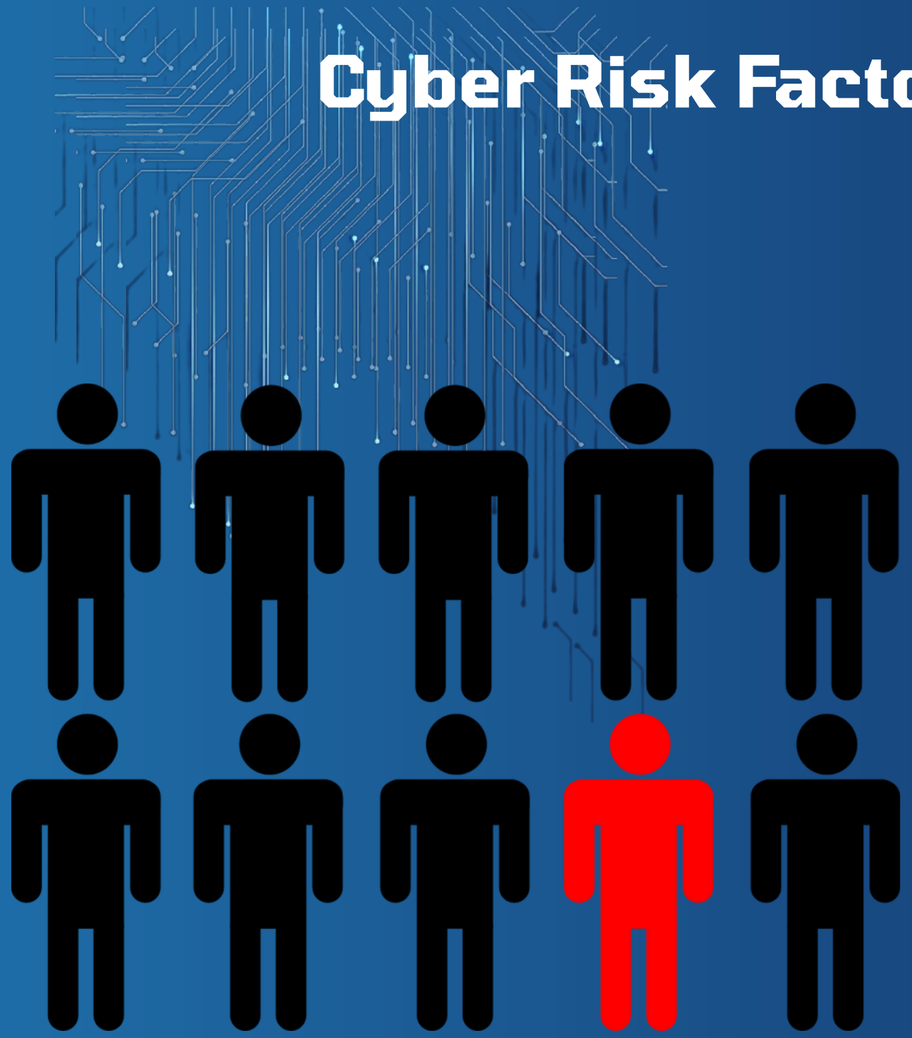
Cyber Risk Factors in Public Financial Operations

INSIDER THREAT



An insider threat refers to a security risk that originates from within an organization, typically involving a current or former employee, contractor, or trusted third party who has or had authorized access to the organization's systems, data, or premises, and uses it, intentionally or unintentionally, to harm the organization

Cyber Risk Factors in Public Financial Operations



MALICIOUS INSIDER

An individual within the organization who deliberately compromises systems or leaks sensitive data for personal gain or to cause harm.

NEGLIGENT INSIDER

An employee who unintentionally puts the organization at risk due to careless or unsafe cybersecurity practices.

COMPROMISED INSIDER

A trusted user whose account has been taken over by an external attacker, often without their knowledge.

Cyber Risk Factors in Public Financial Operations

Insider threats pose significant risks due to the following reasons:

- Government personnel typically have direct access to confidential taxpayer information, procurement files, and disbursement platforms.
- Critical financial systems depend on role-based access, which can be exploited if misused.
- These threats often remain unnoticed for extended periods, particularly when they involve trusted or high-ranking individuals

Cyber Risk Factors in Public Financial Operations

DRIVE-BY ATTACKS

A drive-by download is a type of cyberattack where malicious software is downloaded and installed automatically onto a user's device without their knowledge or consent — just by visiting a compromised or malicious website.

A drive-by download can take advantage of an app, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates.

Cyber Risk Factors in Public Financial Operations

ATTACK PROCESS:

Website Visit – The user unknowingly lands on a compromised legitimate site or a malicious site created by attackers.

Hidden Exploit Activation – The site silently runs malicious code that takes advantage of weaknesses in the user's browser, extensions , or outdated software.

Silent Malware Download – Without any clicks or prompts, malware is automatically downloaded to the user's device.

Malware Deployment – Once installed, the malware can:

- Harvest sensitive information or login credentials
- Create hidden access points
- Install ransomware or spyware
- Connect the infected device to a botnet

Cyber Risk Factors in Public Financial Operations

DRIVE-BY DOWNLOADS ARE PARTICULARLY DANGEROUS BECAUSE:

- A single compromised machine could give attackers access to budget systems, disbursement records, or sensitive taxpayer data
- Malware can spread laterally to other government systems
- It can bypass traditional email-based defenses, entering through web browsing activity

Cyber Risk Factors in Public Financial Operations

Malicious Mobile App

A malicious mobile app is software designed to cause harm to a device or its user. These apps can steal personal information, install malware, or even take control of the device

They often disguise themselves as legitimate apps to trick users into downloading them.

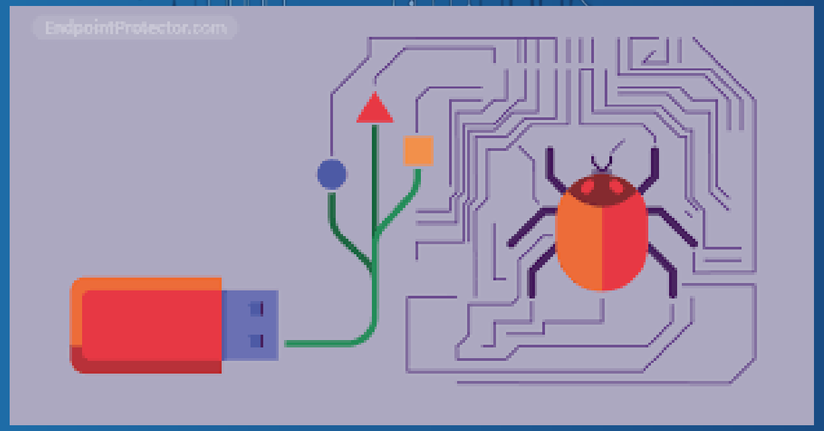
Cyber Risk Factors in Public Financial Operations

Malicious apps can:

- Harvest sensitive information, such as passwords, banking details, or access credentials to government systems
- Monitor user activity by capturing screen content, taking unauthorized photos, or reading private messages
- Take control of the device, allowing attackers to run apps, send messages, or download additional malware remotely
- Infect connected systems, potentially spreading malware to computers or networks when the mobile device is plugged in

Cyber Risk Factors in Public Financial Operations

REMOVABLE MEDIA (USB DEVICES)



MALWARE INFECTION
Attackers can load malware onto USBs that automatically infect office computers, potentially stealing data or opening remote access.

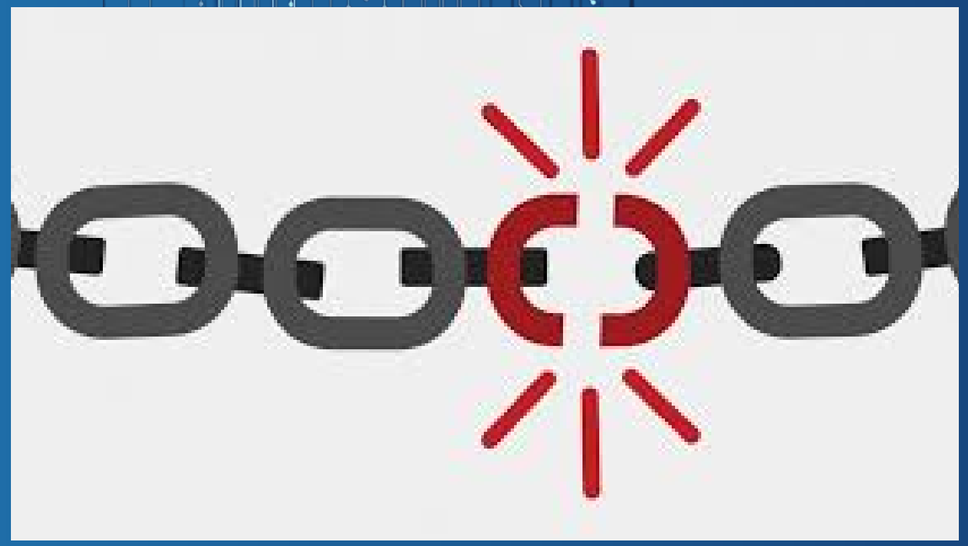
AUTO-RUN EXPLOITS
Outdated systems may run harmful files from USBs without any user action.

QUICK DATA THEFT
Insiders or intruders can use USBs to quickly copy confidential files (budgets, payroll, procurement records).

BYPASSING SECURITY
Because USBs are physical devices, they can sneak past network defenses like firewalls and email filters—especially if security rules are weak

Cyber Risk Factors in Public Financial Operations

Supply Chain Attack



A supply chain attack is a type of cyberattack where an attacker exploits vulnerabilities in a third-party vendor, supplier, or partner's system to gain access to a larger organization's network or data. Instead of directly targeting the main organization, attackers leverage the trust and connections within the supply chain to infiltrate systems

Cyber Risk Factors in Public Financial Operations

SolarWinds is a technology company that creates tools to help large organizations, including government agencies, banks, energy companies, and others, monitor and manage their IT systems.

SolarWinds Experience

- Hackers broke into SolarWinds — the company that makes the software.
- They secretly put a hidden backdoor (a kind of malware) into a regular software update called "Orion."
- SolarWinds sent out this update to all its customers - thinking it was clean.
- Thousands of customers installed the update, including U.S. government agencies, big companies, and security organizations.
- The malware let the hackers quietly sneak into those systems without being noticed.
- The hackers used this access to spy, steal data, and explore systems.

Cyber Risk Factors in Public Financial Operations

INFECTED ORION PLATFORM

One of SolarWinds' most popular products is called Orion. It helps IT departments see all their networks and computers from a single dashboard.

It's like a control center where IT staff can:

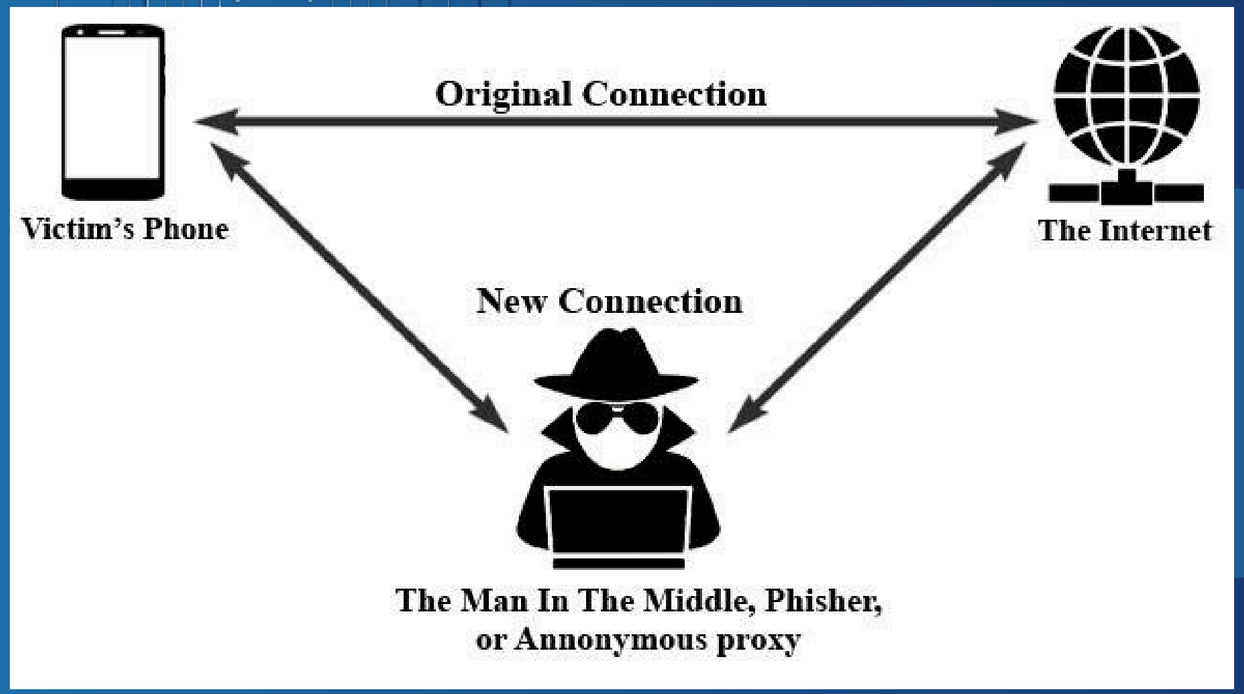
- Spot problems
- Track traffic
- Check if systems are working
- Detect unusual activity

Clients trusted Orion and relied on it heavily to run their daily operations

Because Orion is deeply integrated into IT systems, it has privileged access to network maps, servers, and sensitive data. Thus, compromising Orion means gaining access to everything it can see.

Cyber Risk Factors in Public Financial Operations

Man-in-the-Middle (MitM) Attack



A Man-in-the-Middle (MitM) attack occurs when a cybercriminal quietly intercepts or changes the communication between two parties without either party being aware

Cyber Risk Factors in Public Financial Operations

COMPONENTS OF AN ORGANIZATION'S ATTACK SURFACE FOR MITM

1. Compromised Internal Network (LAN)
Even without Wi-Fi, government offices rely on wired (Ethernet) networks.
A malicious insider or attacker can discreetly plug a rogue device (e.g., mini computer or USB tap) into the network to monitor or tamper with data moving between devices — like between a user's PC and the system of a government agency.
Example: An attacker intercepts credentials or alters fund transfer details between a workstation and a financial system.

2. Malware Inside the Office
Phishing emails or infected USBs can install malware on a staff computer.
This malware can silently act as a middleman, stealing logins, manipulating fund requests, or leaking sensitive documents.
Example: Malware on an accountant's device captures login credentials while accessing the DBM eBudget portal.

Cyber Risk Factors in Public Financial Operations

COMPONENTS OF AN ORGANIZATION'S ATTACK SURFACE FOR MITM

3. Insecure Remote Access / VPN
Remote access setups (especially post-pandemic) may use weak VPNs or unprotected login portals.
Attackers can spoof these systems to trick users into revealing credentials through fake sites.
Example: A government treasurer connects to a fake COA portal and unknowingly submits sensitive login information.

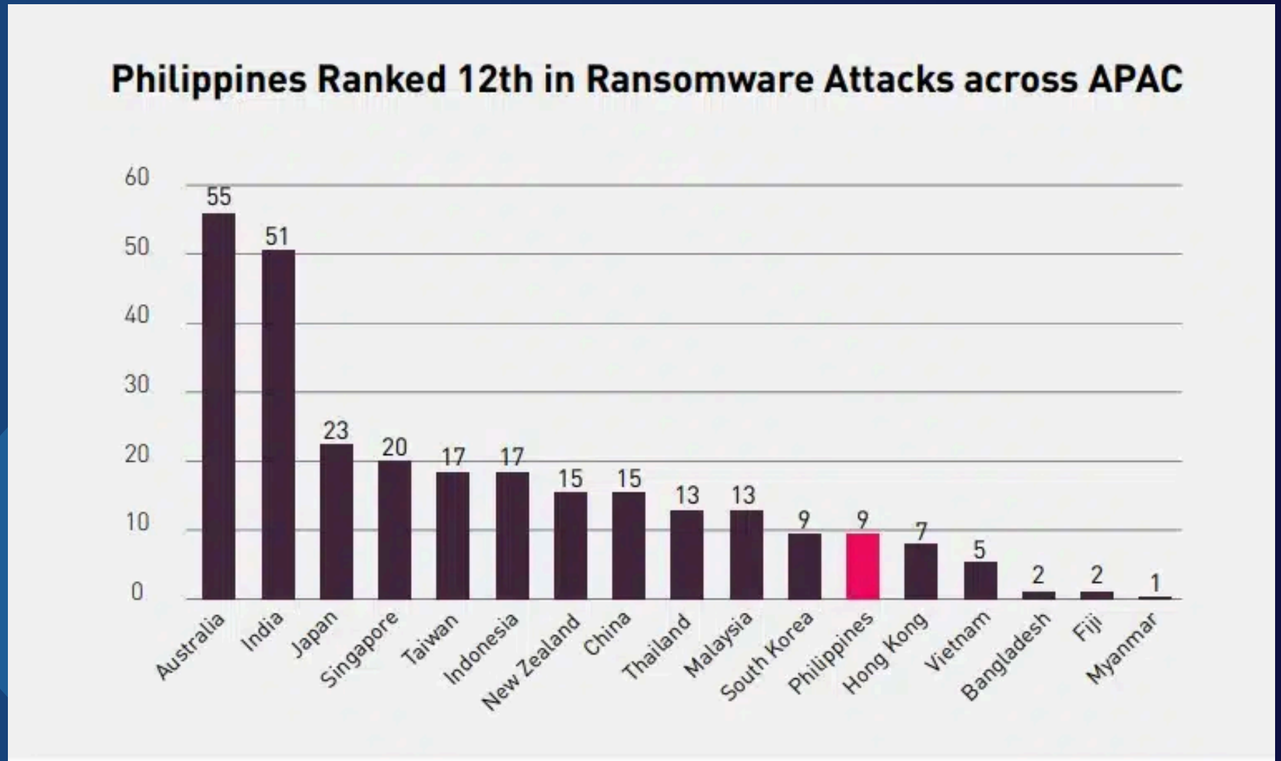
4. Mobile Hotspots and Tethering
When official networks are unavailable, staff may tether devices to mobile data.
Attackers can mimic mobile or Wi-Fi networks to intercept connections and capture data.
Example: A field officer connects to a fake "SmartGovPH" Wi-Fi hotspot, allowing an attacker to spy

Cyber Risk Factors in Public Financial Operations

RANSOMWARE ATTACK

A ransomware attack is a type of cyber incident where malicious software encrypts a victim's files or locks their system, making it unusable until a ransom is paid, typically in cryptocurrency.

Cyber Risk Factors in Public Financial Operations



PH Ransomware 2023 2024

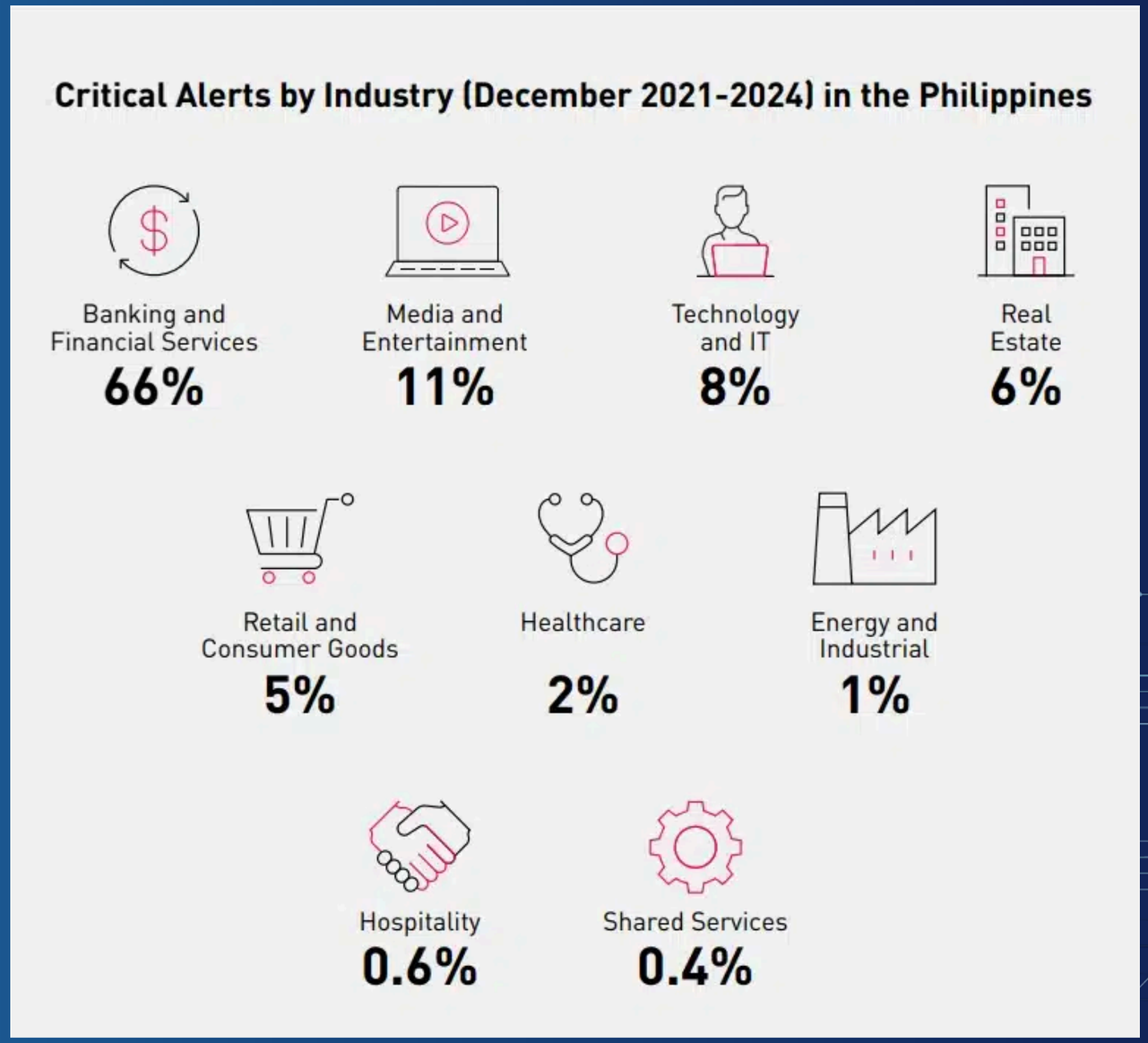
2023	2024
20	9

The Philippines will likely not be targeted as much as developed countries in 2024.

The motives of the majority of Local Threat Actors will still stay the same:
Hacktivism, Ideology, and Personal Satisfaction.

Ransomware is still not in the plans of local threat actors.

Cyber Risk Factors in Public Financial Operations



STRENGTHENING GOVERNMENT CYBERSECURITY: PREVENTION AND INCIDENT MITIGATION

STRENGTHENING GOVERNMENT CYBERSECURITY: PREVENTION AND INCIDENT MITIGATION

THE NCSP (2023–2028) TARGETS THREE MAIN OUTCOMES:

Proactive Cybersecurity Protection – Securing government networks, enhancing the National Computer Emergency Response Team (NCERT), and establishing a National Security Operations Center.

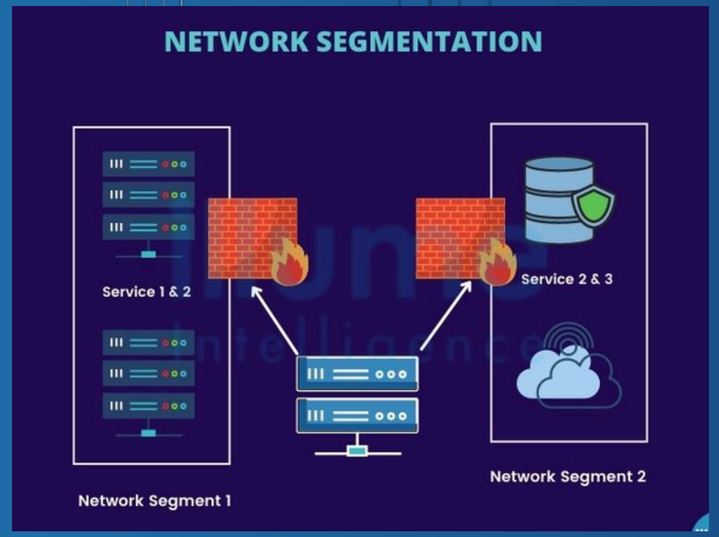
Stronger Cybersecurity Workforce – Providing scholarships, international certifications, and re-establishing the ICT Academy to build skilled professionals.

Improved Policy Framework – Strengthening coordination through the National Cybersecurity Inter-Agency Committee (NCIAC), pushing for an executive order on Critical Information Infrastructure (CII) protection, and advocating new laws.

STRENGTHENING GOVERNMENT CYBERSECURITY: OPERATIONALIZING CYBERSECURITY IN DAILY GOVERNMENT FUNCTIONS

- Secure internal systems by applying proper network segmentation, firewalls, antivirus, and intrusion detection systems.
- Conduct regular vulnerability assessments and penetration testing.
- Ensure all systems are updated and patched to prevent exploitation of known vulnerabilities.

STRENGTHENING GOVERNMENT CYBERSECURITY: OPERATIONALIZING CYBERSECURITY IN DAILY GOVERNMENT FUNCTIONS



Network Segmentation

- Divide networks into secure zones
- Isolate sensitive systems
- Limit internal access

Network segmentation means breaking your network into zones. HR, finance, and public-facing systems should be isolated to prevent lateral movement if one is compromised.

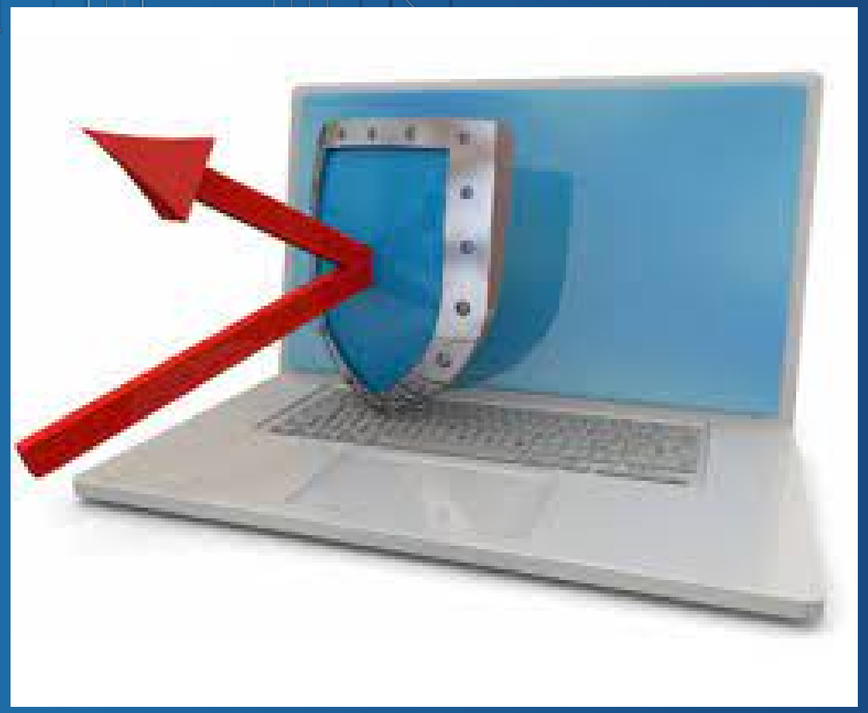
STRENGTHENING GOVERNMENT CYBERSECURITY: OPERATIONALIZING CYBERSECURITY IN DAILY GOVERNMENT FUNCTIONS

Firewalls

- Controls incoming/outgoing traffic
- Applies at network edges and internally
- Enforces security policies

Firewalls are like digital gates. They inspect traffic and block harmful or unauthorized access. Every agency must configure them properly for both external and internal protection

STRENGTHENING GOVERNMENT CYBERSECURITY: OPERATIONALIZING CYBERSECURITY IN DAILY GOVERNMENT FUNCTIONS



Antivirus and Endpoint Protection

- Protects individual devices
- Detects and neutralizes malware
- Should update and scan regularly

STRENGTHENING GOVERNMENT CYBERSECURITY: OPERATIONALIZING CYBERSECURITY IN DAILY GOVERNMENT FUNCTIONS

Intrusion Detection Systems/Intrusion Protection System

- Monitors network for attacks
- Alerts staff to anomalies
- Supports real-time detection
- Takes action (IPS) — such as:
  - Blocking malicious IP addresses
  - Dropping harmful network packets
  - Terminating dangerous user sessions
  - Sending alerts

STRENGTHENING GOVERNMENT CYBERSECURITY: OPERATIONALIZING CYBERSECURITY IN DAILY GOVERNMENT FUNCTIONS

Vulnerability Testing

- Find system weaknesses
- Simulate real-world attacks
- Patch issues before exploitation

Identifies flaws before attackers do. This is part of a proactive defense posture.

STRENGTHENING GOVERNMENT CYBERSECURITY: OPERATIONALIZING CYBERSECURITY IN DAILY GOVERNMENT FUNCTIONS

STRENGTHEN CYBERSECURITY INFRASTRUCTURE

System Updates and Patch Management

- Set up centralized patch management tools
- Schedule regular maintenance windows to apply updates.
- Keep an inventory of software used to ensure all systems are patched.

Applying updates to fix security flaws in software and systems.

STRENGTHENING GOVERNMENT CYBERSECURITY: DEVELOPING CYBERSECURITY COMPETENCE

Develop and Strengthen Cybersecurity Competence

- Provide cybersecurity training and awareness programs for both IT and non-IT employees.
- Collaborate with accredited institutions to offer certified courses aligned with national standards.
- Foster a workplace culture that emphasizes cybersecurity awareness

STRENGTHENING GOVERNMENT CYBERSECURITY:ADOPTION OF UNIFIED CYBERSECURITY POLICIES

ADOPT UNIFIED CYBERSECURITY POLICIES

- Implement internal procedures that reflect the national security framework.
- Designate a Cybersecurity Officer to ensure compliance and coordination efforts

STRENGTHENING GOVERNMENT CYBERSECURITY:ADOPTION OF UNIFIED CYBERSECURITY POLICIES

Legal and Regulatory Justification

In the context of national governance and public sector accountability, the establishment of unified cybersecurity policies and designated leadership is not merely strategic — it is a legal and regulatory necessity.

- Under the Data Privacy Act of 2012 (RA 10173), all government agencies and private entities handling personal data are mandated to implement appropriate organizational, physical, and technical security measures.

- The DICT's National Cybersecurity Plan (NCSP 2023–2028) requires the institutionalization of agency-level cybersecurity frameworks that adhere to national and sectoral standards.

STRENGTHENING GOVERNMENT CYBERSECURITY:ADOPTION OF UNIFIED CYBERSECURITY POLICIES

KEY INTERNAL PROCEDURES TO ALIGN WITH NATIONAL STANDARDS:

- Passwordless authentication / enforce strong passphrase policies with MFA
- Access control levels (who can access what)
- Incident response and reporting procedures
- Data protection and privacy compliance

STRENGTHENING GOVERNMENT CYBERSECURITY: SAFEGUARDING OF CRITICAL INFORMATION INFRASTRUCTURE (CII)

SAFEGUARD CRITICAL INFORMATION INFRASTRUCTURE (CII)

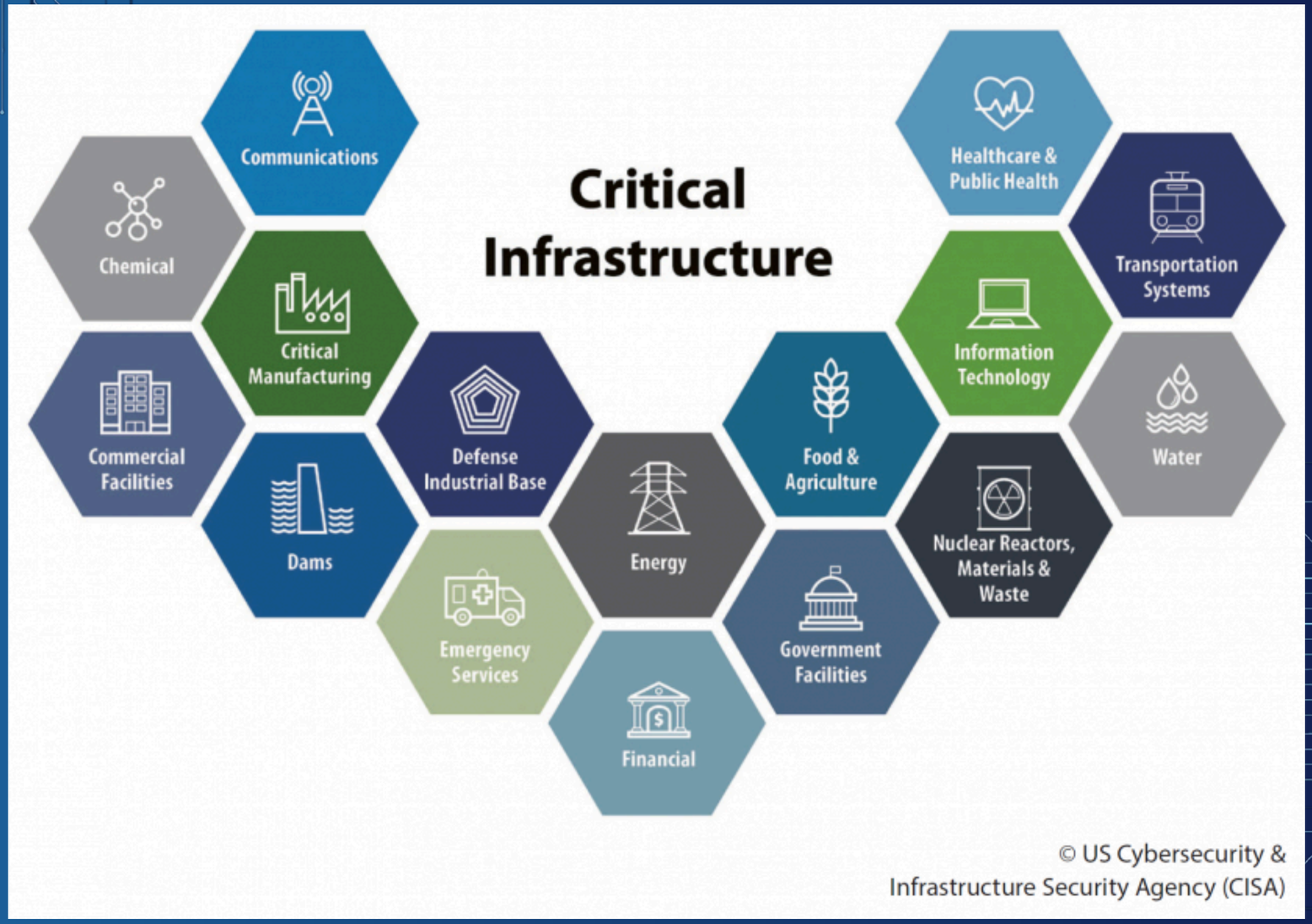
- Determine if your systems or data are classified as CII and apply necessary enhanced safeguards.
- Enforce strict access controls, ensuring only authorized personnel can access critical systems and data

STRENGTHENING GOVERNMENT CYBERSECURITY:SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE (CII)

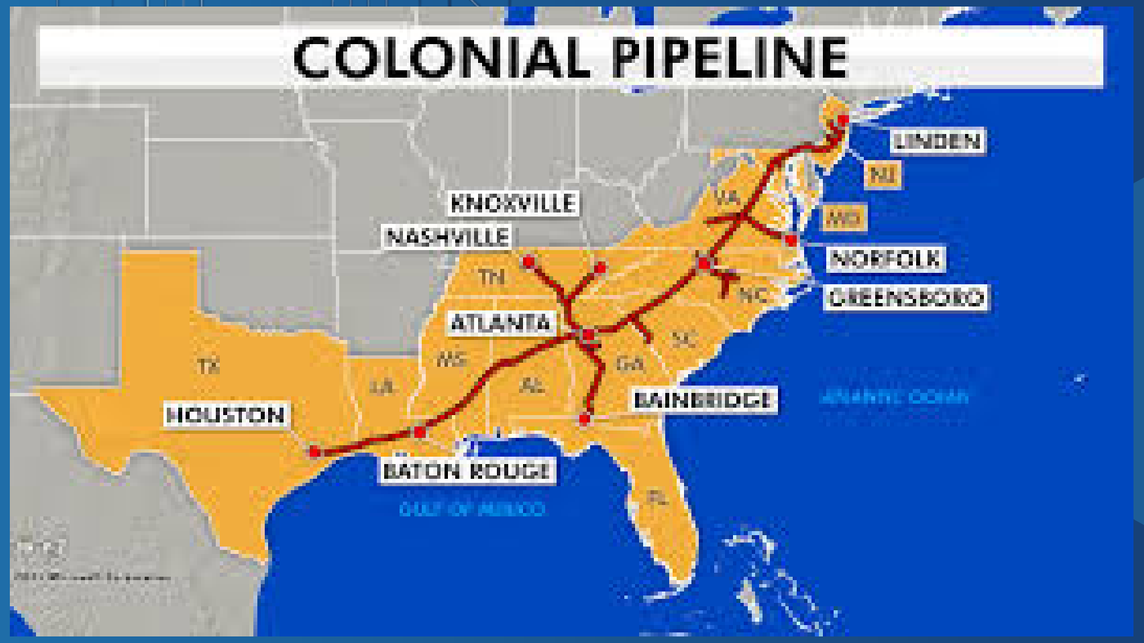
Critical Inrastructure - A set of systems and assets that are essential to a nation such that any disruption of their service can have a serious impact on national security, economy, social well-being, and citizen safety. - *NCSP 2023 -28*

Critical Information Infrastructure - Consists of information process and Information Communications Technology which form part of the operation of the Critical Infrastructures (CI). - *NCSP 2023-28*

STRENGTHENING GOVERNMENT CYBERSECURITY:SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE (CII)



STRENGTHENING GOVERNMENT CYBERSECURITY:SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE (CII)



- A ransomware group (DarkSide) hacked into Colonial Pipeline's IT systems using stolen credentials.
- Operations were shut down for several days, cutting off fuel supply to the U.S. East Coast.
- Gas shortages, panic buying, price spikes
- Company paid $4.4 million in ransom

STRENGTHENING GOVERNMENT CYBERSECURITY:SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE (CII)

WHAT IS ACCESS CONTROL?

Access control is a security measure that determine who can access what data or systems, and under what conditions. They are essential for limiting exposure to unauthorized users, both from inside and outside government institutions

STRENGTHENING GOVERNMENT CYBERSECURITY:SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE (CII)

Key Practices Under Access Control

Role-Based Access Control (RBAC)
Assign permissions based on the employee's role.
Example: A procurement officer cannot access HR records; a finance officer cannot modify IT systems.

Multi-Factor Authentication (MFA)
Combine passwords with a second factor like biometrics or one-time PINs.
The NCSP encourages MFA across all agencies, especially for accessing email, databases, and cloud services.

Privileged Access Management (PAM)
Limit high-level access (e.g., admin accounts) to a few trusted individuals.
Monitor the use of such accounts to detect misuse or unusual activity.

Regular Access Reviews
Conduct scheduled reviews to ensure only current and authorized staff have system access.
Remove accounts of resigned, retired, or transferred employees immediately.

STRENGTHENING GOVERNMENT CYBERSECURITY:SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE (CII)

Significance of Access Control

- Prevents insider threats/misuse of data by employees
- Reduces exposure from compromised credentials
- Helps trace accountability in case of a data breach.
- Complies with national mandates under the NCSP and proposed cybersecurity legislation.

STRENGTHENING GOVERNMENT CYBERSECURITY:STRENGTHEN INCIDENT RESPONSE AND REPORTING

STRENGTHEN INCIDENT RESPONSE AND REPORTING

- Collaborate with the National Computer Emergency Response Team (NCERT) during incidents.
- Develop and regularly test a formal Incident Response Plan (IRP).
- Ensure timely and accurate reporting of cyber incidents to national authorities

STRENGTHENING GOVERNMENT CYBERSECURITY:STRENGTHEN INCIDENT RESPONSE AND REPORTING

- The NCERT, under the National Cybersecurity Inter-Agency Committee (NCIAC), was created through Executive Order No. 189.
- Pursuant to EO 189, the NCERT shall issue guidelines on the handling of government data/information by members of Computer Emergency Response Teams (CERTs) to be organized within the respective agencies and shall perform oversight and audit functions as to compliance with said guidelines.
- Republic Act No. 10844 transferred the functions related to cybersecurity, including those of the NCERT, to the Department of Information and The National Cybersecurity Plan 2023–2028 explicitly calls for the reorganization and strengthening of NCERT.
- NCSP envisions to expand NCERT to allow it to operate nationwide with the capability to respond on-premise should a major cybersecurity incident is reported

STRENGTHENING GOVERNMENT CYBERSECURITY:STRENGTHEN INCIDENT RESPONSE AND REPORTING

Significance of an Incident Response Plan

- Minimize damage from cyberattacks (financial, reputational, operational)
- Contain the threat quickly before it spreads
- Ensure business continuity and fast recovery
- Comply with regulations

STRENGTHENING GOVERNMENT CYBERSECURITY:STRENGTHEN INCIDENT RESPONSE AND REPORTING

TIME AND ACCURACY IN REPORTING

MITIGATION OF HARM AND CONTAINMENT OF THREATS

- Facilitates the swift containment of cyber threats, thereby minimizing potential damage to information systems and critical infrastructure.

PROTECTION OF INTERCONNECTED GOVERNMENT SYSTEMS

- Early notification assists in alerting other agencies to similar or evolving threats. This supports the proactive defense of the broader public sector ecosystem.

PRESERVATION OF DIGITAL EVIDENCE

- Timely incident documentation ensures the availability of relevant forensic data necessary for technical analysis, attribution, and potential legal proceedings.

ACCURACY AND COMPLETENESS OF INFORMATION

- Allows authorities to assess the scale and nature of the threat, determine systemic vulnerabilities, and implement appropriate remedial and preventive measures.

STRENGTHENING GOVERNMENT CYBERSECURITY: INTEGRATION OF CYBERSECURITY IN ALL PROJECTS

INTEGRATE CYBERSECURITY BY DESIGN IN ALL PROJECTS

- Incorporate security assessments and planning in every digital transformation project—from e-governance platforms to automated payroll systems.
- Demand cybersecurity compliance from third-party vendors, ensuring that all contracts include data protection clauses and security obligations

Cybersecurity is not an afterthought, but a built-in requirement from the beginning of every digital project.

SIGNIFICANT CYBERSECURITY LAWS

SIGNIFICANT CYBERSECURITY LAWS

[EXECUTIVE ORDER NO. 29, June 01, 2023]
STRENGTHENING THE INTEGRATION OF PUBLIC FINANCIAL MANAGEMENT INFORMATION SYSTEMS, STREAMLINING PROCESSES THEREOF, AND AMENDING EXECUTIVE ORDER NO. 55 (S. 2011) FOR THE PURPOSE

Executive Order No. 29, s. 2023 directs all national government agencies to harmonize and integrate their financial management systems such as budgeting, accounting, and cash management under a unified framework to improve transparency, auditability, and operational efficiency.

It establishes a governance mechanism to resolve fragmentation and mandates the use of shared standards, with DICT providing infrastructure and cybersecurity support

SIGNIFICANT CYBERSECURITY LAWS

DIGITIZATION REQUIRES CYBERSECURITY

- EO 29 mandates the implementation of the Integrated Financial Management Information System (IFMIS) across national government agencies.
- As financial processes shift to digital platforms—budgeting, cash management, accounting—the risk of cyber threats increases significantly.
- Financial managers must therefore understand and enforce cybersecurity controls to protect these systems.

SIGNIFICANT CYBERSECURITY LAWS

CONCENTRATION OF FINANCIAL DATA

- IFMIS centralizes vast amounts of financial information, including budget execution and cash flows.
- This centralization increases the attack surface for potential data breaches or ransomware.
- Strong cybersecurity measures, such as encryption, access control, and audit logging, are essential to secure this data

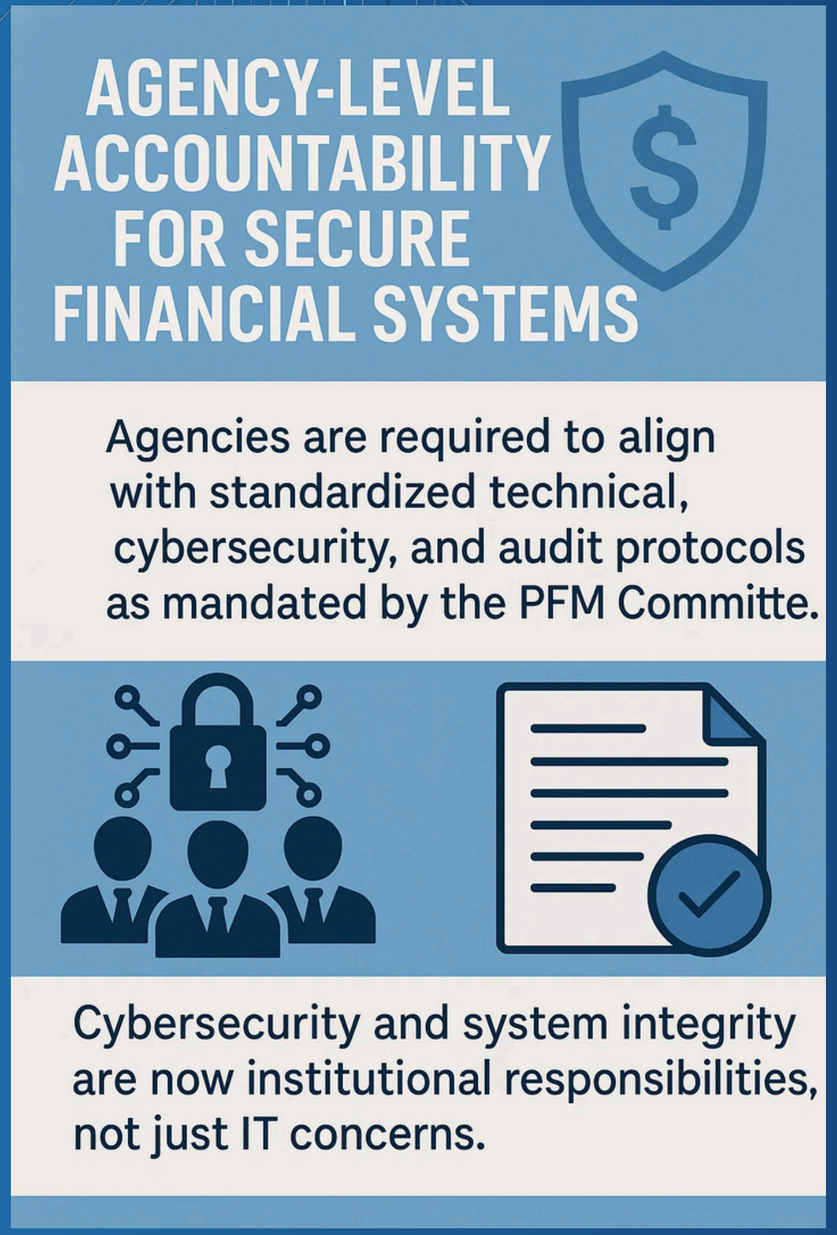
SIGNIFICANT CYBERSECURITY LAWS

CLEAR MANDATE FOR SECURITY SUPPORT

EO 29 explicitly tasks the Department of Information and Communications Technology (DICT) with providing technical and policy support.

This inclusion signals that cybersecurity is not optional. It is embedded in the design and implementation of modern financial systems.

SIGNIFICANT CYBERSECURITY LAWS



Agency-Level Accountability for Secure Financial Systems

- Agencies are required to align with standardized technical, cybersecurity, and audit protocols as mandated by the PFM Committee.
- Cybersecurity and system integrity are now institutional responsibilities, not just IT concerns

SIGNIFICANT CYBERSECURITY LAWS

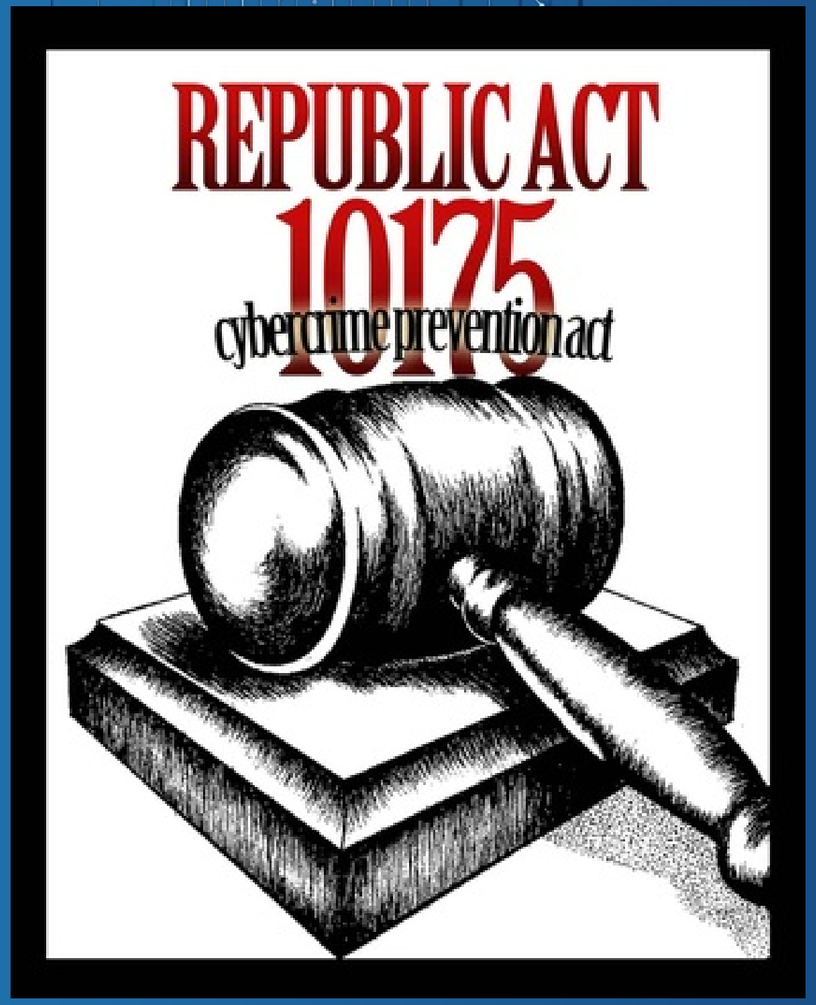
PREPARATION FOR INCIDENT RESPONSE

As digital finance operations increase, so do the risks of data leaks, fraud, and hacking.

EO 29's integration with cybersecurity principles supports the need for government agencies to have proper incident response plans and threat monitoring.

SIGNIFICANT CYBERSECURITY LAWS

CYBERCRIME PREVENTION ACT



OFFENSES AGAINST CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS

- Illegal access
- Illegal interception
- Data Interference
- System Interference
- Misuse of Devices
- Cyber Squatting

COMPUTER-RELATED OFFENSES

- Computer-related forgery
- Computer-related Fraud
- Computer-related Identity Theft

CONTENT-RELATED OFFENSES

- Cybersex
- Child Pornography
- Unsolicited Commercial Communications
- Libel

SIGNIFICANT CYBERSECURITY LAWS

REAL-TIME COLLECTION OF TRAFFIC DATA (SECTION 12)

What It Allows:
Law enforcement may collect real-time traffic data related to electronic communications using technical means.

Traffic data includes only metadata like:

- Origin and destination
- Route
- Time, date, size, and duration
- Type of service

Content of messages or personal identities is excluded,

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information

SIGNIFICANT CYBERSECURITY LAWS

Traffic data refers to technical details about an electronic communication. It includes:

- Origin – the source (e.g., sender's IP address)
- Destination – the intended receiver (e.g., recipient's IP or email)
- Route – the network path it travels
- Time and date – when the communication occurred
- Size – the amount of data sent
- Duration – how long it lasted
- Type of service – what kind of communication it was (e.g., email, file transfer, messaging)

These details help track how and when communication happened, but not what was actually said or shared.

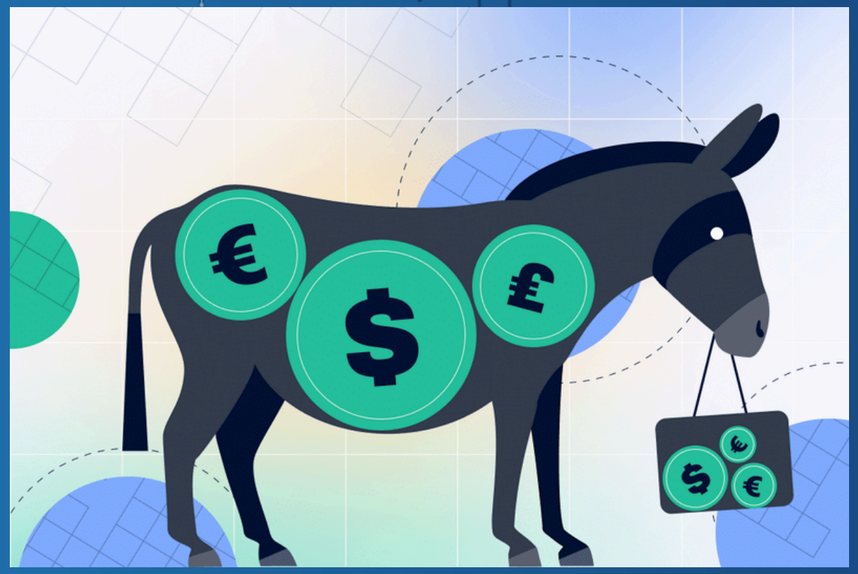
SIGNIFICANT CYBERSECURITY LAWS

RA 12010 (ANTI-FINANCIAL ACCOUNT SCAMMING ACT)

- Protect the Financial System: The law aims to safeguard the integrity and stability of the Philippine financial system by deterring and preventing the use of financial accounts for illicit activities.
- Safeguard Individuals: AFASA seeks to empower individuals by providing them with tools and resources to recognize and prevent scams, while also holding perpetrators accountable for their actions.
- Enhance Digital Financial Security: Recognizing the increasing reliance on electronic commerce and digital financial services, the Act emphasizes the importance of securing these platforms and ensuring responsible digital financial practices. AFASA seeks to foster a secure and trustworthy digital financial ecosystem

SIGNIFICANT CYBERSECURITY LAWS

MONEY MULING ACTIVITIES



- This prohibited act involves using, borrowing, or allowing the use of a Financial Account to obtain, receive, deposit, transfer, or withdraw proceeds known to be derived from crimes, offenses, or social engineering schemes.
- Recruiting, enlisting, contracting, hiring, utilizing, or inducing any person to perform these acts is also penalized.
- Money mules are individuals who unknowingly or intentionally facilitate the movement of illicit funds through their accounts, often acting as intermediaries in financial scams.

SIGNIFICANT CYBERSECURITY LAWS

SOCIAL ENGINEERING SCHEMES

Social engineering schemes are committed by individuals who obtain sensitive identifying information of another person through deception or fraud, resulting in unauthorized access and control over the person's Financial Account.

These schemes often involve exploiting human trust and vulnerabilities to gain access to personal information.

SIGNIFICANT CYBERSECURITY LAWS

ECONOMIC SABOTAGE

The prohibited acts under Section 4(a) and (b) shall be considered as economic sabotage when committed under any of the following circumstances:

(1) By a group of three (3) or more persons conspiring or confederating with one another;
(2) Against three (3) or more persons individually or as a group;
(3) Using a mass mailer; or
(4) Through human trafficking

SIGNIFICANT CYBERSECURITY LAWS

Other Offenses. - The following shall also constitute as offenses under RA 12010

(a) Willfully aiding or abetting in the commission of any of the offenses enumerated under Section 4;
(b) Willfully attempting to commit any of the offenses enumerated under Section 4;
(c) Opening a Financial Account under a fictitious name or using the identity or identification documents of another; or
(d) Buying or selling a Financial Account.

SIGNIFICANT CYBERSECURITY LAWS

"Section 12. Investigation and Inquiry into Financial Accounts. - The BSP shall have the authority to investigate and inquire into Financial Accounts which may be involved in the commission of a prohibited act or offense under Sections 4 and 5 hereof. The provisions of Republic Act No. 1405, as amended; Republic Act No. 6426, as amended; Republic Act No. 8367; and Republic Act No. 10173 shall not apply to Financial Accounts subject of BSP's investigation.

Any of the information gathered from the investigation or inquiry of a Financial Account by the BSP pursuant to this section may be used for the enforcement of this Act and in the implementation of relevant provisions of Republic Act No. 11765.

The authority to investigate and inquire into Financial Accounts under this section shall be exercised by a duly authorized officer or body from the BSP.

No court below the Court of Appeals shall have jurisdiction to enjoin the BSP from exercising its authority to investigate and inquire into any Financial Account under this Act.

An Institution, or any of its directors, officers, or employees, shall be held free and harmless from any accountability or liability for any act done in compliance with an order from the BSP for an inquiry or investigation of a Financial Account."

SIGNIFICANT CYBERSECURITY LAWS

"Section 14. Sharing of Information of Financial Accounts. - The BSP shall have the authority to issue rules on information-sharing and disclosure with law enforcement and other competent authorities in connection with its inquiry and investigation of Financial Accounts under this Act: Provided, That any information on the Financial Account which may be shared by BSP shall be used solely to investigate and prosecute cases involving violations of Section 4 and 5 of this Act and to implement the relevant provisions of Republic Act No. 11765.

Section 15. Prohibition on the Disclosure of Information of a Financial Account. - Unless otherwise allowed under existing laws, directors, trustees, officers, or employees of an Institution, government officials or employees, or other persons who obtained information on the Financial Account subject of BSP's inquiry or investigation under this Act, shall be prohibited from disclosing such information on the Financial Account for purposes other than those mentioned in Section 12 and 14 hereof."

SIGNIFICANT CYBERSECURITY LAWS

CIVIL LIABILITY: RECTIFICATION AND COMPENSATION

"Section 17. Civil Liability in Case of Conviction. - A conviction for violation of this Act shall carry with it civil liability, which may include restitution for the damage done in favor of the aggrieved party of any unwarranted benefit derived from such violation.

Independent of a criminal case, all properties, tools, instruments and/or any other non-liquid assets used for the commission of the acts prohibited in Sections 4 and 5 of this Act shall be subject to civil forfeiture, upon finding of probable cause, in accordance with rules of procedure to be formulated by the Supreme Court: Provided, That in cases of economic sabotage as defined in Section 4(c), the rules shall include a summary procedure for the release of a portion of such assets during the pendency of the proceedings, for operational support and victim protection, including victims of human trafficking involved in the commission of prohibited acts and other offenses in this Act."

SIGNIFICANT CYBERSECURITY LAWS

THE DATA PRIVACY ACT (RA 10173)

- Setting rules on how personal data must be collected, stored, processed, and disposed of whether by government or private institutions.
- Requiring transparency, legitimate purpose, and proportionality in data handling.
- Mandating safeguards (technical and organizational) to prevent unauthorized access, breaches, or misuse of personal information.
- Holding institutions accountable for data protection and requiring breach notifications and compliance with the National Privacy Commission (NPC).
- Balancing privacy rights with the need for efficient public service, law enforcement, and economic development.

SIGNIFICANT CYBERSECURITY LAWS

KEY OBLIGATIONS OF PERSONAL INFORMATION CONTROLLERS (PICS):

- Implement organizational, physical, and technical safeguards. Protect against destruction, alteration, disclosure, unlawful processing
- Address natural and human threats (accidental loss, unauthorized access, data breaches, etc.)
- Align security measures with nature of data, risk level, agency size and best practices

SIGNIFICANT CYBERSECURITY LAWS

Security Obligations of Government Agencies and Third-Party Contractors

Heads of government agencies are accountable for ensuring that sensitive personal information in their custody is secured using appropriate industry standards as recommended by the National Privacy Commission (NPC). The NPC is tasked with monitoring compliance and may issue corrective recommendations to meet minimum security standards. *(Sec. 22, RA 10173)*

Government contractors handling sensitive personal information from 1,000 or more individuals must register their data processing systems with the NPC and fully comply with all applicable data privacy requirements, just as government agencies and personnel must. *(Sec. 24, RA 10173)*

KEY TAKEAWAYS

1. Cybersecurity as a Fiscal Duty
   - Safeguarding public funds extends beyond the prevention of fraud; it includes the obligation to maintain the confidentiality, integrity, and availability of digital systems that manage budgeting, disbursement, and financial reporting.

2. Legal Compliance as Operational Imperative
   - Republic Acts No. 10175, 10173, and 12010 collectively strengthen the protection of public funds by penalizing cyberattacks and financial scams (RA 10175 and RA 12010) and by requiring secure, lawful, and accountable processing of personal and financial data (RA 10173)

3. Harmonized Policies as Risk Mitigation
   - A unified cybersecurity policy framework across government entities promotes operational clarity, fortifies institutional resilience, and facilitates timely and coordinated responses to cyber incidents.

4. Security by Design as a Mandated Principle
   - Cybersecurity must be embedded from the conceptualization phase of all digital initiatives—including e-payroll systems, procurement platforms, and financial applications—ensuring that contracts with third-party vendors contain enforceable data protection provisions.

KEY TAKEAWAYS

5. Preparedness and Incident Management
   - All government offices must establish, implement, and regularly test an Incident Response Plan. Prompt reporting of cybersecurity incidents to the National Computer Emergency Response Team (NCERT) or the appropriate authority is essential to contain threats and mitigate damage.

6. Role of Leadership in Cybersecurity Governance
   - Financial managers must serve as cybersecurity stewards upholding compliance, advancing cyber hygiene awareness, and fostering coordination between technical and administrative units to enforce controls.

7. Ensuring Public Confidence through Secure Systems
   - Cybersecurity breaches may not only disrupt public service delivery but also erode institutional trust. Citizens have a legitimate expectation of transparency and data protection in all government digital transactions.

INVESTING IN DIGITALIZATION WITHOUT SHORING UP CYBERSECURITY PRACTICES IS AS MISGUIDED AS BUILDING A HOUSE WITHOUT A FOUNDATION. - Jesper Zerlang