



# INFORMATION ASSURANCE AND SECURITY

Information Assurance and  
Security 1

Introduction to  
Information Assurance and  
Security **01**

**02** Tenets of Information  
Systems Security


Philippine Compliance  
Laws about Information  
Assurance and Security **03**

**04** International Compliance  
Laws about Information  
Assurance and Security

# 01

## INTRODUCTION TO INFORMATION ASSURANCE AND SECURITY





**WHY IS THERE A  
NEED FOR  
ORGANIZATIONS  
TO HAVE  
INFORMATION  
SECURITY?**

# AXIE INFINITY

## Axie Infinity hack highlights DPRK cryptocurrency heists

The \$620 million hack of developer Sky Mavis earlier this year is only the latest in a long line of cryptocurrency platform attacks conducted by North Korean nation-state actors.



By Alexander Culafi, News Writer

Published: 18 May 2022

Despite how enormous it was, the Axie Infinity heist marked only the latest chapter in the story of North Korean financial cybercrime.

Sky Mavis, the developer of popular nonfungible token (NFT) video game Axie Infinity, lost hundreds of millions of dollars in assets [when they were stolen](#) by hackers on March 23. The attack occurred via a breach of the Ronin bridge that exists as part of the Ronin Network sidechain (also developed by Sky Mavis).

The breach occurred when attackers gained control of a series of validator nodes attached to Axie Infinity to conduct fake withdrawals. Hackers stole 173,600 Ethereum and 25.5 million USD Coin, worth approximately \$620 million at the time (and about \$375 million as of this writing).

Three weeks after the initial attack and two weeks after it was disclosed, the FBI [formally attributed](#) the attack to the Lazarus Group and APT38, nation-state threat groups tied to the North Korean government.

Whitepapers, events, social...

Which resources  
do you turn to on  
your pre-purchase  
research?

TAKE THE SURVEY



### Sponsored News

Defeating Ransomware With Recovery From Backup  
—Exagrid

Unlock the Value Of Your Data To Harness Intelligence and Innovation  
—HPE

Modernizing Cyber Resilience Using a Services-Based Model  
—Dell Technologies

See More

Related Content

# LAPSUS\$

## Everything We Learned From the LAPSUS\$ Attacks

May 12, 2022 The Hacker News



In recent months, a cybercriminal gang known as LAPSUS\$ has claimed responsibility for a number of high-profile attacks against technology companies, including:

- T-Mobile (April 23, 2022)
- Globant
- Okta
- Ubisoft
- Samsung
- Nvidia
- Microsoft
- Vodafone

# US COLONIAL PIPELINE

## Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad



Photographer: Samuel Corum/Bloomberg

By William Turton and Kartikay Mehrotra

June 5, 2021 at 3:58 AM GMT+8

• LIVE ON B  
Watch Live  
Listen to L

# INFORMATION ASSURANCE



Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.



“Information assurance is the confidence that the information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.”

–HMG Strategy

# INFORMATION SECURITY

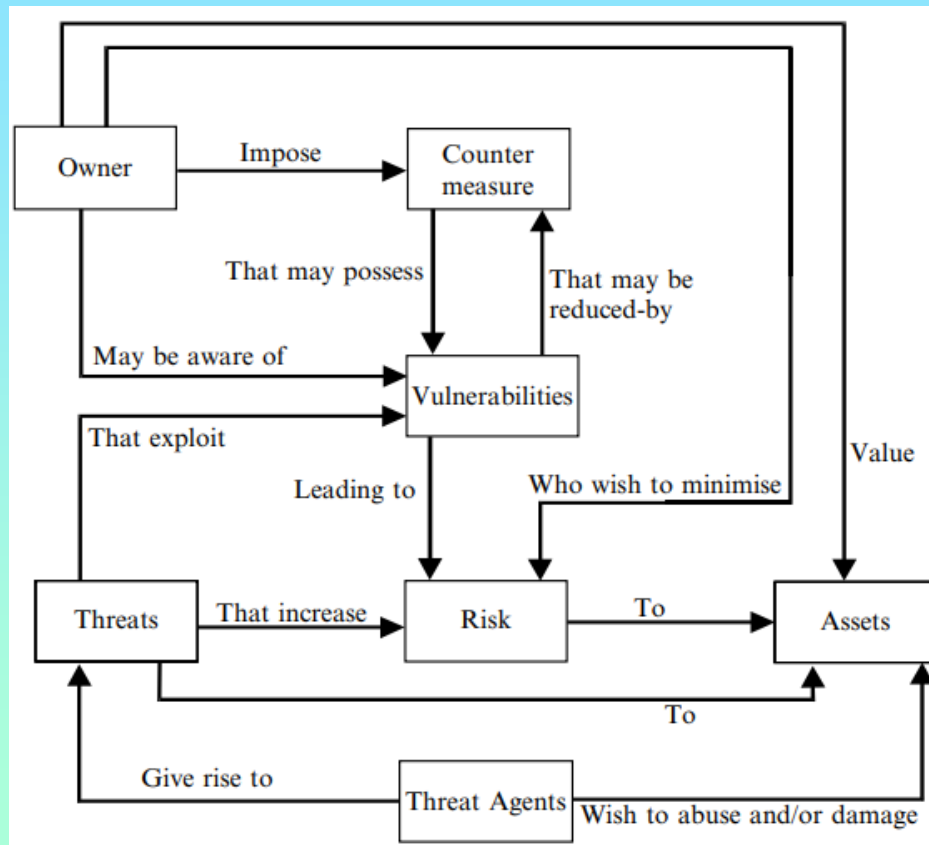


The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

“Information Security is the preservation of confidentiality, integrity and availability of information.”

– BS7799/ISO17799

# INFORMATION ASSURANCE AND SECURITY IN CONTEXT



# 02

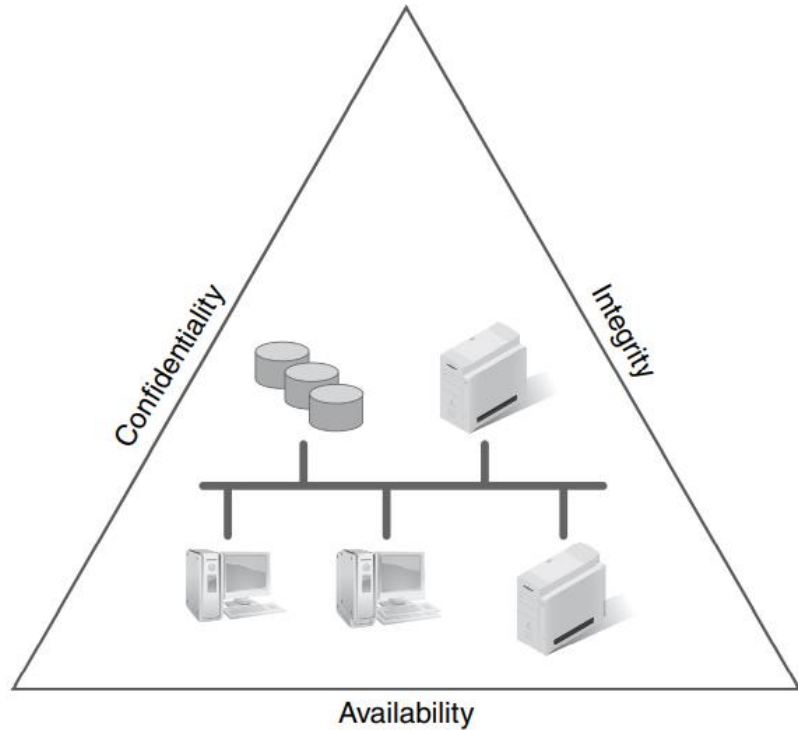
## TENETS OF INFORMATION SYSTEMS SECURITY





**HOW CAN WE  
PROTECT OUR  
INFORMATION  
FROM RISKS?**

# TENETS OF INFORMATION SECURITY



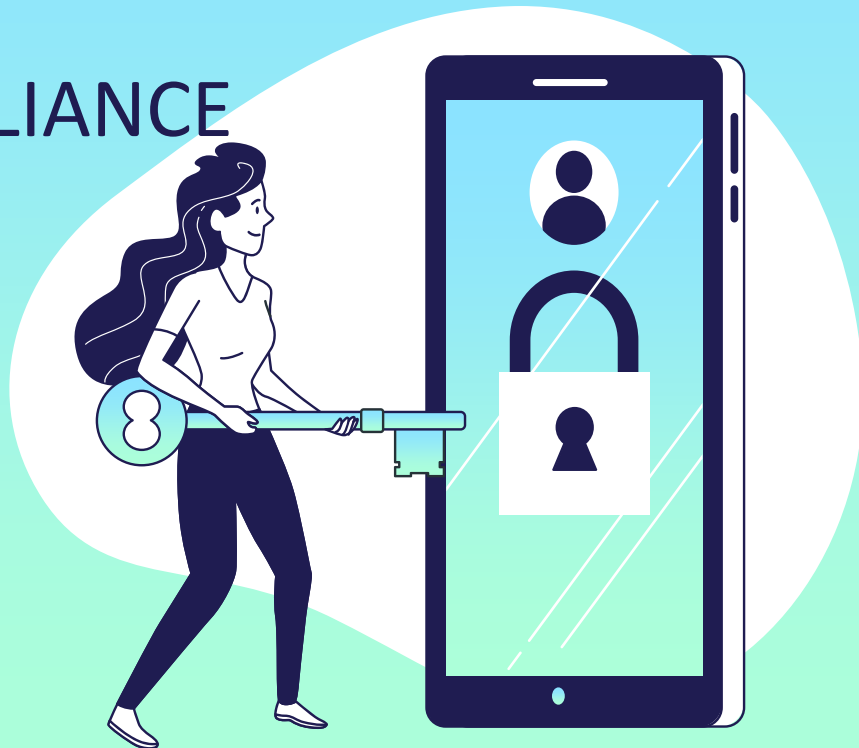
**Confidentiality** is a common term. It means guarding information from everyone except those with rights to it.

**Integrity** deals with the validity and accuracy of data. Data lacking integrity—that is, data that are not accurate or not valid—are of no use.

**Availability** is generally expressed as the amount of time users can use a system, application, and data.

# 03

## PHILIPPINE COMPLIANCE LAWS ABOUT INFORMATION ASSURANCE AND SECURITY





# HOW DOES THE PHILIPPINE GOVERNMENT PROTECT YOUR INFORMATION?



# PHILIPPINE COMPLIANCE LAW: CYBERCRIME PREVENTION ACT OF 2012

The Cybercrime Prevention Act of 2012 (CPA) defines the following as cybercrimes(RA 10175):



- offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices and cybersquatting);
- computer-related offences (computer-related forgery, computer-related fraud and computer-related identity theft); and
- content-related offences (cybersex, child pornography, unsolicited commercial communications and libel).

# PHILIPPINE COMPLIANCE LAW: ELECTRONIC COMMERCE ACT OF 2000



The Electronic Commerce Act of 2000 (ECA) provides for the legal recognition of electronic documents, messages and signatures for commerce, transactions in government and evidence in legal proceedings (RA 8792)

- ECA penalises hacking and piracy of protected material, electronic signatures and copyrighted works
- limits the liability of service providers that merely provide access
- prohibits persons who obtain access to any electronic key, document or information from sharing them

# PHILIPPINE COMPLIANCE LAW: ACCESS DEVICE REGULATION ACT OF 1998



The Access Devices Regulation Act of 1998 (ADRA) penalises various acts of access device fraud, such as using counterfeit access devices (RA 8484).

- Access device is defined as any card, plate, code, account number, electronic serial number, personal identification number or other telecommunications service, equipment or instrumental identifier, or other means of account access that can be used to obtain money, goods, services or any other thing of value, or to initiate a transfer of funds

# PHILIPPINE COMPLIANCE LAW: DATA PRIVACY ACT OF 2012



Data Privacy Act of 2012 (DPA) regulates the collection and processing of personal information in the Philippines and of Filipinos, including sensitive personal information in government(RA 10173).

- created the National Privacy Commission (NPC) as a regulatory authority
- requires personal information controllers to implement reasonable and appropriate measures to protect personal information and notify the NPC and affected data subjects of breaches
- penalises unauthorised processing, access due to negligence, improper disposal, processing for unauthorised purposes, unauthorised access or intentional breach, concealment of security breaches and malicious or unauthorised disclosure in connection with personal information.



## INTERNATIONAL STANDARDS ADOPTED BY PHILIPPINES

- The DICT Memorandum Circular No. 5 (2017) required government agencies to adopt the Code of Practice in the Philippine National Standard (PNS) ISO/IEC 27002 (Information Technology – Security Techniques – Code of Practice for Information Security Controls) by 14 September 2018
- CII to implement the PNS on Information Security Management System ISO/IEC 27001 by 14 September 2019
- Non-CII sectors may voluntarily adopt PNS ISO/IEC 27002
- DICT conducts risk and vulnerability assessment based on ISO 27000 and ISO 31000 and security assessment based on ISO/IEC TR 19791:2010 of CIIs at least once a year
- DICT also issues a Certificate of CyberSecurity Compliance to CIIs based on ISO/IEC 15408 (Information Technology – Security Techniques – Evaluation Criteria for IT Security) and ISO/IEC 18045 (Methodology for IT Security Evaluation)

## ● INTERNATIONAL STANDARDS ADOPTED BY PHILIPPINES

- DICT Circular No. 2017-002 includes ISO/IEC 27001 as an accepted international security assurance control for verifying data that can be migrated to GovCloud or the public cloud
- ISO/IEC 17203:2011 Open Virtualization Format specification as a standard for interoperability of GovCloud workloads.

# 04

## INTERNATIONAL COMPLIANCE LAWS ABOUT INFORMATION ASSURANCE AND SECURITY





# WHAT INTERNATIONAL LAWS ARE BEING USED TO PROTECT USERS?



# INTERNATIONAL STANDARDS FOR INFORMATION ASSURANCE AND SECURITY

- The ISO/IEC 270001 family of standards, also known as the ISO 27000 series, is a series of best practices to help organizations improve their information security.
- ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)
- ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization
- ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector.

# INTERNATIONAL STANDARDS FOR INFORMATION ASSURANCE AND SECURITY

- ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
- ISO/IEC TR 19791:2010 provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408 by taking into account a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation
- ISO/IEC 18045:2008 is a companion document to ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security. ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408
- ISO/IEC 17203:2011 specifies an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.

**THANK YOU**