Unidades de Informática

Forense

Armando Diaz

Objetivos de esta presentación

Cybercrimen costs

Standards and guidelines for digital forensics laboratories

Dominican Republic Overview

Trends

¿El costo del cibercrimen?

Cybercrime is predicted to cost the world $8 trillion USD in 2023, according to Cybersecurity Ventures. If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China. Press Release

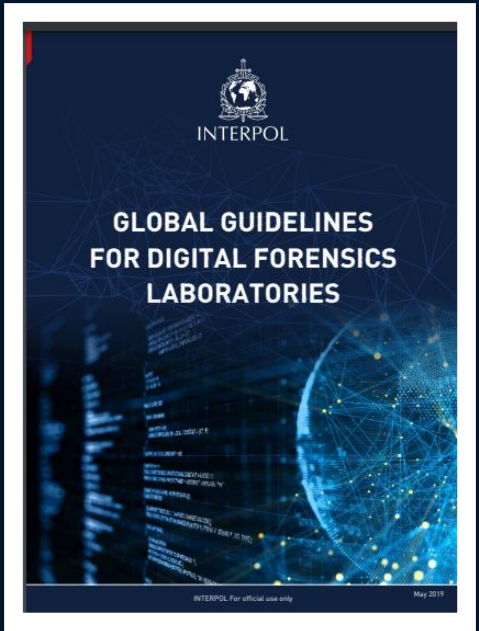
That report provides a breakdown of the cybercrime damage costs predicted in 2023:

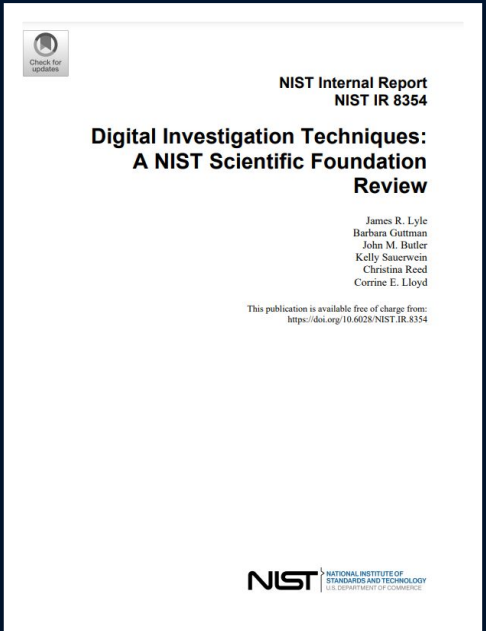
- $8 trillion USD a Year.
- $667 billion a Month.
- $154 billion a Week.
- $21.9 billion a Day.
- $913 million an Hour.
- $15.2 million a Minute.
- $255,000 a Second.

$$B_m + B_p > C_c + C_f P_a P_c$$

B_m	Beneficio monetario del atacante
B_p	Beneficio psicologico del atacante
C_c	Costo para cometer el crimen
C_f	Costo monetario de fallo y condena del atacante
P_a	Probabilidad de ser arrestado
P_c	Probabilidad de condena

- Clark and Davis 1995





2.8.5 Standards Organizations

Some standards organizations, e.g., American Society for Testing and Materials (ASTM) International and International Organization for Standardization (ISO), produce standards for digital forensics. Standards organizations usually require a fee to obtain a copy of a standard. Some ASTM Standards related to digital forensics include:

- E2678-09(2014) Standard Guide for Education and Training in Computer Forensics
- E2825-19 Standard Guide for Forensic Digital Image Processing
- E2916-19e1 Standard Terminology for Digital and Multimedia Evidence Examination
- E3016-18 Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis
- E3017-19 Standard Practice for Examining Magnetic Card Readers
- E3046-15 Standard Guide for Core Competencies for Mobile Phone Forensics
- E3115-17 Standard Guide for Capturing Facial Images for Use with Facial Recognition Systems
- E3148-18 Standard Guide for Postmortem Facial Image Capture
- E3149-18 Standard Guide for Facial Image Comparison Feature List for Morphological Analysis
- E3150-18 Standard Guide for Forensic Audio Laboratory Setup and Maintenance
  Some ISO digital forensics standards include:
- ISO/IEC 27041:2015 — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method
- ISO/IEC 27042:2015 — Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043:2015 — Information technology — Security techniques — Incident investigation principles and processes
- ISO/IEC 27050:2018-2021 — Information technology — Security techniques — Electronic discovery (parts 1 through 4 published)

Ataques cibernéticos en la República Dominicana

Ataques cibernéticos en República Dominicana aumentan un 46% durante la pandemia

Por Dolfi Gómez — 21 julio, 2020 en Tecnología

Hackers atacan el IAD; piden unos US$600 mil para devolverle datos

EL PAÍS

Troi Orlando Espejo
24 agosto, 2022

El Instituto Agrario Dominicano (IAD) está paralizado por los hackers.

Gobierno informa que hackers atacaron 14 de sus páginas web

Artículo

Santo Domingo, RD.

La Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) y el Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT-RD), del Centro Nacional de Ciberseguridad (CNCS), informaron que 14 páginas web del Estado dominicano fueron hackeadas este domingo por el grupo de hackers denominado "Hunter Bajwa Pakistan Zindabad".

La información fue dada a conocer a través de una nota de prensa sin especificar cuáles portales web fueron afectados.

La OGTIC expresó que de un total de 46 sitios web del Gobierno que comparten la misma infraestructura de alojamiento, sólo fueron afectadas esa cantidad por un incidente conocido técnicamente como "Defacement".

Este ataque de desconfiguración de la estructura web, es "el menor que consiste en el aprovechamiento de vulnerabilidades no identificadas en los manejadores de contenido para cambiar la apariencia de un portal web determinado con el propósito de llamar la atención por parte de quien lo realiza".

De acuerdo al Gobierno, el incidente fue mitigado por el equipo del departamento de seguridad de la información de la Oficina Gubernamental de Tecnología de la Información y Comunicación en coordinación con el Equipo Nacional de Respuesta a Incidente Cibernéticos (CSIRT-RD) del Centro Nacional de Ciberseguridad.

- Ataques de botnets en abril de 2020 que aumentaron un 382% en relación al mes anterior
- Ataque de ransomware Quantum al Instituto Agrario Dominicano en agosto de 2022 que afectó múltiples servicios y estaciones de trabajo
- Detección de un inusual incremento en los ataques cibernéticos a las instituciones públicas en enero de 2021 por parte del Centro Nacional de Ciberseguridad de República Dominicana.
- Ataques cibernéticos perpetrados por hackers rusos y chinos en diciembre de 2020 que se prevé que aumenten en el país.

“How to ensure interagency cooperation, and how to avoid conflicting competencies in the field of digital forensics.”

Definición de Marco legal con roles, alcance y responsabilidades. (Ley 53-07, que establece las responsabilidades de cada uno y los medios y mecanismos de intercambio)

Protocolos de cooperación Inter agencial definidos y efectivos en la práctica. (LEA y CSIRT con fines forense e investigación)

Limitations

Recursos Limitados: Las unidades de informática forense enfrentan limitaciones de recursos, incluido el personal insuficiente y la falta de equipo y tecnología actualizada.

Marco Legal y Normativo: En algunos países, el marco legal y normativo relacionado con la evidencia digital puede no existir, no estar actualizado o ser ambiguo, lo que dificulta la presentación de pruebas electrónicas en los tribunales.

Desafíos

Los dispositivos y los algoritmos de cifrado son cada vez más seguros
Aumento dramático en el volumen de evidencia digital
No hay suficiente mano de obra y los retrasos crecen constantemente
El enfoque de fuente única ya no funciona
Problemas de colaboración y trabajo remoto.

Anonimacion

Volatilidad de la evidencia digital

TRENDS

Global ransomware damage costs were predicted to reach $20 billion annually in 2021, up from $325 million in 2015, which is a 57X increase. In a decade from now, the costs will exceed $265 billion.

—Global ransomware damage costs are predicted to exceed $265 billion by 2031

Total global data storage is projected to exceed 200 zettabytes by 2025. This includes data stored on private and public IT infrastructures, on utility infrastructures, on private and public cloud data centers, on personal computing devices — PCs, laptops, tablets, and smartphones — and on IoT (Internet-of-Things) devices.

—World will need to cyber protect 200 zettabytes of data by 2025

We estimate the world will need to secure 338 billion lines of new software code in 2025, up from 111 billion lines of new code in 2017, based on 15 % year-over-year growth in new code.

—World will need to secure 338 billion lines of new software code in 2025

Ransomware attacks continue to increase at an alarming rate. Data from Verizon discovered a 13% increase in ransomware breaches year-over-year. Ransomware attacks have also become increasingly targeted — sectors such as healthcare and food and agriculture are just the latest industries to be victims, according to the FBI.

—Ransomware-as-a-Service is here to stay

Amateurs hack systems,
Professionals hack people.

Bruce Schneier

MUCHAS GRACIAS