precision CYBERTECHNOLOGIES & DIGITAL SOLUTIONS

CYBER DIGITAL WORLD

NEWSLETTER

Volume 2: Issue No. 1 **October:** 2021

Cybersecurity Awareness Month

Dr. Ronald Walcott
Managing Director

Every year since 2003, October has been recognized as National Cyber Security Awareness Month (NCSAM). This effort was brought to life through a collaboration between the U.S. Department of Homeland Security and the National Cyber Security Alliance. NCSAM was created to ensure that every individual stay safe and secure online. The theme for 2021 is 'Do Your Part. #BeCyberSmart', helping to empower individuals and organizations to own their role in protecting their part of cyberspace. Are you cyber-smart and what does that mean?

National Cybersecurity Awareness Month has grown into a global effort, with both individuals and organizations taking part — and for good reason. Cyber-attacks continue to dominate tech headlines because of the far-reaching impact they have on everyone from everyday internet users to businesses and governments. The latest findings from IBM's Cost of a Data Breach report shows the average cost to organizations at an all-time high, totaling US$4.24 million.

In our last issue, we stressed the importance of employee awareness and we also discussed best practices to assist with ransomware. Continuing from our last issue, some other ways employees can protect against ransomware include:

- Back up files
- Educate end users
- Use an intrusion detection system
- Whitelist applications
- Provide limited privilege
- Use email filtering

WHAT IS THE CIA TRIAD IN CYBERSECURITY?

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.

Confidentiality

The confidentiality of information is often the first aspect of cybersecurity considered, certainly when it comes to many high-profile 'hacks'

In this Issue:

that are reported in the headlines. When a nefarious actor gains unauthorized access to an organization's user data, such as emails or payment information, this is a compromise of confidentiality.

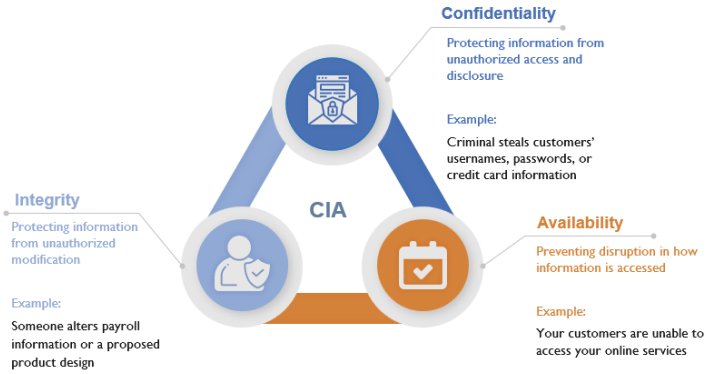
Integrity

Both the accuracy and completeness of information are integral to an organizations ability to function. Integrity focuses on ensuring that data has not been tampered with and that it can be trusted as authentic and reliable.

It should be noted that integrity isn't just about protecting data whilst being stored, but also whilst it is being used, and whilst in transit. As with the confidentiality of information, integrity relies on both encryption and hashing, as well as employing other processes such as digital signatures, intrusion detection systems and stringent organizational procedures.

Availability

As you can assume, the value of information reduces dramatically if users or an organization cannot access it. Put simply, availability is that the networks and systems



are functioning properly, and authorized parties can access resources, data and information, as and when they are needed.

Whilst a great deal of availability is reliant on the maintenance of digital systems, those digital systems are also reliant upon physical preconditions, and thus availability is dependent upon consistent power, a lack of human errors and the functionality of hardware.

HEADLINE NEWS:

White House to host virtual ransomware summit with 30 countries - but not Russia

One major topic of conversation will be how countries can cooperatively trace and disrupt criminal use of cryptocurrencies like Bitcoin

One major topic of conversation will be how countries can cooperatively trace and disrupt criminal use of cryptocurrencies like Bitcoin

The Biden administration is set to host a two-day virtual ransomware summit starting Wednesday, the largest international gathering of its kind to date, with one notable absence: Russia was not invited. The White House plans for at least 30 countries to attend a series of meetings to be held over Zoom. The summit will be the most concrete step it has taken so far to build an international coalition to address ransomware, an epidemic of cybercrime where hackers remotely lock victims' computers and demand an extortion payment to fix them.\

Ransomware cost victims an estimated $74 billion in total damages last year, according to a study by the cybersecurity firm Emsisoft. While the U.S. has the most known cases, the problem is global: At least eight other countries suffered more than a thousand known ransomware attacks in 2020.

After hackers attacked a major oil pipeline owner and meat processor earlier this year, the White House launched a multi-pronged effort to confront ransomware, including sanctioning a cryptocurrency exchange that allegedly helped hackers launder their extorted bitcoins into cash.

Biden said he told Russian President Vladimir Putin during a June meeting that ransomware attacks from Russian citizens against U.S. critical infrastructure were off-limits. The White House has since cautioned that it would take months to see if such conversations will prove effective.

Jen Easterly, the director of the Cybersecurity and Infrastructure Security Agency, said last week that Russian ransomware hackers have yet to make "any significant, material changes" to their usual rapid pace of attacks.

Source: https://news.yahoo.com/white-house-host-virtual-ransomware-090016080.html

Frequently Asked Questions:

WHAT IS THE POSSIBLE IMPACT OF RANSOMWARE?

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

WHAT DO I DO IF I BELIEVE MY SYSTEM HAS BEEN INFECTED BY RANSOMWARE?

Signs your system may have been infected by Ransomware:

- Your web browser or desktop is locked with a message about how to pay to unlock your system and/or your file directories contain a "ransom note" file that is usually a .txt file
- All of your files have a new file extension appended to the filenames

Examples of Ransomware file extensions: .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .LeChiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .HA3, .toxcrypt, .magic, .SUPERCRYPT, .CTBL, .CTB2,

Upcoming Events

VIRTUAL CYBERSECURITY SUMMIT SOUTH AFRICA
October 27, 2021

CYBERSECURITY SUMMIT: NEW YORK
November 9, 2021

VIRTUAL CYBERSECURITY SUMMIT INDIA & SAARC: ZERO TRUST
November 16, 2021

VIRTUAL CYBERSECURITY & FRAUD SUMMIT: FRANCE
November 23, 2021

Source: https://www.databreachtoday.com/events

868-610-7237

salesinfo@precision-cyber.com

www.precision-cyber.com

1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad