Security Assessment of an Enterprise' E-mail and Domain Name System: A Case Study

Dr. Eric B. Blancaflor, Eduardo Jose P. Del Rosario, Kent Andrei Dominique M. Tan, Lance Michael A. Delariarte, Christian Earl A. Santos and David Allan R. Uy
School of Information Technology
Mapua University, Makati, Philippines
ebblancaflor@mapua.edu.ph, ejpdelrosario@mymail.mapua.edu.ph,
kadmtan@mymail.mapua.edu.ph, lmadelariarte@mymail.mapua.edu.ph,
ceasantos@mymail.mapua.edu.ph, daruy@mymail.mapua.edu.ph

Abstract

The domain name system (DNS) is a critical protocol in today's Internet operation. It establishes a standard naming convention for human-readable, understandable, and memorable domain names and IP addresses of Internet services. The abundance of study on DNS in general and security and privacy suggests that all issues in this area have been resolved. The reality, however, is that despite the substantial amount of literature on different elements of DNS, there are still many unresolved issues. The researchers offered a standards-based security assessment using Cyber Security Evaluation Tool (CSET) to help the staffing agency understand and assess the many hazards associated with using the domain name system. Furthermore, the researchers investigate a range of potential countermeasures to such threats.

Keywords
DNS, IP Address, threats, security assessment, CSET

1. Introduction

A program must be launched to discover vulnerabilities that hostile actors may exploit. Vulnerability is defined as the lack or weakness of a safeguard in an asset or resource. This lack or deficiency increases the potential for danger or assault to be more damaging or expensive, as well as more likely to occur (Newman, R.C. 2006). Deadly network security assaults may take the form of computer viruses, which can quickly propagate across networked systems. Viruses can damage data, destroy files, slow down system operations by spawning bogus processes, and prevent programs from storing information.

In this case study, the researchers performed a comprehensive cybersecurity assessment using CISA.gov Cyber Security Evaluation Tool. CSET can:

- Provide a consistent means of evaluating a control system network as part of a comprehensive cybersecurity assessment
- Specify cyber security recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture

IT Security Officers and IT Network Specialists are the type of participants to use this evaluation tool to assess the organization/enterprise cybersecurity posture. The users may choose a maturity model based on the kind of organization/enterprise. A maturity model is a method for evaluating the effectiveness of an organization in achieving a specific goal. Additionally, it may assist an organization in identifying where its practices are lacking or ineffective and where they are deeply ingrained in the company. In cyber security, a maturity model is a tool that may be used to track the development of an organization's security integration into its daily and strategic operations and the progress of similar businesses within an industry.

1.1 Objective of the Study

The approach was made by evaluating the current configuration digital infrastructure, with a cursory understanding of the network and operations of a Home Healthcare Staffing Agency. The researchers are not permitted to conduct exploits on any of the company's assets. This is to prevent the agency's activities from being disrupted. The researchers followed these high-level stages:

- Assess the Google Admin e-mail configuration
- Assess the virtual server's network configuration
- Specify cybersecurity recommendations
- Harden the e-mail security configuration

1.2 Scope and Limitation

The evaluation was restricted to the following scope: Google Admin Console (Google Workspace), GoDaddy Registrar, Cloudflare DNS and Digital Ocean Droplet. The assessment approach has no specified limits. The agency's Administrator simply needed the security researchers to guarantee that no operations would be interrupted during working hours. The network restored all systems to their former state following the scan.

2. Review of related literature and studies

The researchers frame the study on Enterprise E- mail and Domain Name System vulnerabilities. Security procedures were examined.

2.1 An e-mail is an essential form of communication to organizations.

Due to the critical nature of e-mail in the business community, significant research has been conducted to analyze and investigate e-mail services to understand better the threat these services may pose and provide the best possible solutions for securing e-mail services (Kour, J., & Ahmed, H. 2020). In 2018, a study was performed to look at e-mail spoofing. It investigated how e-mail providers recognize these e-mails and how they end up in consumers' inboxes. According to the study findings, using specific security extensions such as SPF, DKIM, and DMARC in an adequately configured manner may help avoid or mitigate these threats (Hu, H. & Wang, G. 2018).

2.2 Cybersecurity principles for healthcare organizations and agencies.

Investment in modern IT infrastructure with efficient patch management and malware prevention is critical for minimizing actions in both healthcare and academic contexts. Additionally, institutions should educate all staff about common cyber-attacks, which include (1) tricking victims into downloading malicious apps, (2) phishing e-mails masquerading as official outbreak updates that distribute malware via attachments or links, and (3) embedding spyware or malware in publicly available interactives. Maps and webpages for COVID-19 (Europol 2020). Second, proper 'cyber-hygiene should be integrated into employees' daily work routines. This involves the following: (1) using solid passwords; (2) avoiding unfamiliar e-mails and links; (3) enabling firewall protection at work and home; and (4) providing good employee training (Infosec 2020).

Healthcare institutions should be aware of the extra hazards associated with any cyber-attack and take necessary measures to mitigate them (Infosec 2020). Due to healthcare facilities' underinvestment in cyber security, some are especially susceptible to ransomware attacks, notably during the COVID-19 epidemic. Cybercriminals may disable devices, servers, or whole networks and demand a ransom payment to decrypt the data. This may disrupt patient data, imaging and surgical procedures, medical equipment, and appointment scheduling systems. As medical equipment becomes more 'connected,' cybercriminals may hack devices like cardiac pacemakers (Healthinformatics UIC 2020). Healthcare facilities should remember that any cyber-security compromise may result in the exposure of personally identifiable medical information and can significantly disrupt clinical services, including emergency or life-saving treatment, culminating in death. Institutions must be prepared to deal with the immediate and long-term consequences of any assault, taking economic and legal considerations into account. They must have robust business continuity strategies in place (Bhuyan SS, Kabir U, Escareno JM, et al. 2020).

Additionally, they should foster a security culture among workers by ensuring that all personnel gets cyber- security training. A highly educated and responsive cyber- security staff should be immediately accessible, and companies should guarantee that access to electronic health record systems is audited meticulously. All mobile devices that hold confidential medical information should be encrypted, and employees should not install software without prior approval. Employees remotely working should connect to a virtual private network (VPN) to maintain a secure connection across insecure internet infrastructure (Bhuyan, SS, Kabir U, Escareno JM, et al. 2020).

3. Methodology

The researchers believed that assessing an organization's security posture via the use of a Cyber Security Evaluation Tool (CSET) from CISA would offer a systematic, disciplined, and repeatable method. The researchers assessed Account Management, Boundary Protection, Firewall, Audit and Accountability, Organizational Management, Access Control, Physical Security, Information Protection, System Integrity, and Monitoring & Malware.

The agency provided the researchers with a copy of their network diagram, as shown in Figure 1, to help them search for network and infrastructure vulnerabilities.

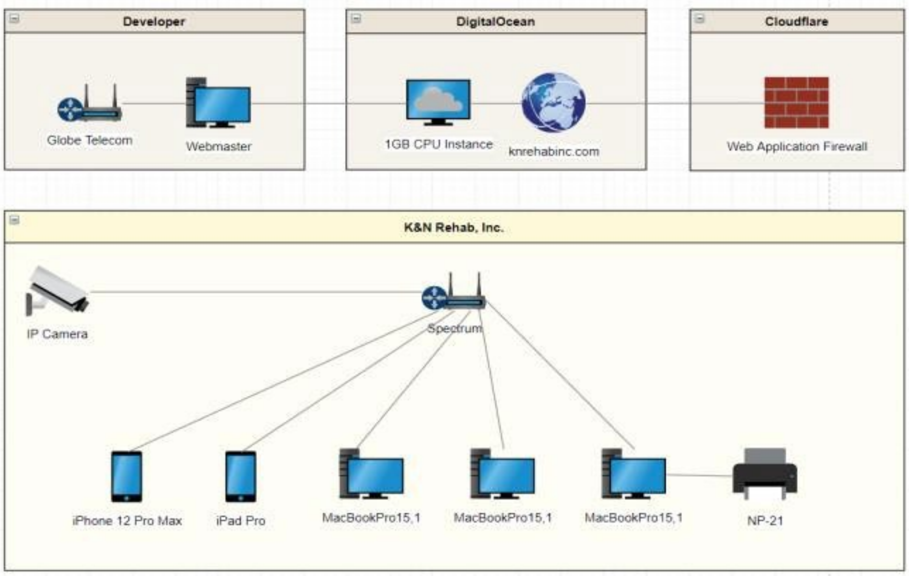


Figure 1. Network Diagram

3.1 The Assessment Process

3.1.1 Select standard

Users are encouraged to choose one or more of the government- and industry-recognized cybersecurity standards listed below. The CSET then produces questions that are tailored to those specifications.

3.1.2 Determine Assurance Level

The security assurance level (SAL) is calculated by users' answers to questions about the possible implications of a successful cyberattack on an ICS organization, facility, system, or subsystem. CSET then calculates a SAL and recommends the appropriate degree of cybersecurity rigor to guard against a worst-case scenario. CSET conducts a comparison analysis between the requirements specified in the chosen standards and the responses given by the user, using the SAL to establish the necessary degree of security (NCCIC, n.d.). In this research, the overall values in the confidentiality resulted as moderate, in integrity is high and in availability is low. Table 1 shows the series of questions used in this study to assess the Security Assurance Level.

Table 1. Security Assurance Level Questionnaire

Diagram Component Questions
Account Management
Are accounts locked after a defined number of failed login attempts?
Boundary Protection
Are public-facing servers placed in a DMZ? In other words, behind a firewall with an additional firewall between that and any systems on the internal network?

Are loose and strict source routing blocked and logged?
Has the egress firewall rules for the outbound traffic from the control network been reviewed and implemented?
Have rule sets been checked for appropriate order?
Have state tables been reviewed?
Is all incoming and outgoing ICMP traffic denied except where expressly permitted by your organization?
Is direct external traffic, traffic from the Internet, to critical servers blocked by default?
Is traffic to your e-mail server only allowed via a specific protocol and port?
Firewall
Does the firewall ruleset include an allowlist of approved users access, e.g., IP address restrictions, all others are refused?
Does the firewall support Denial of Service (DoS) protection?
Logging
Do logs get archived securely on another host for offline analysis?
Are events, such as failed login attempts and failed file system actions, logged?
Are system administrators automatically notified of potential security threats, e.g., failed login attempts, failed file system activity, and malformed URL requests?
Does logging include, but is not limited to critical host file changes, unauthorized and authorized client connection activity, and ad- hoc network creation?
Are authentication and administrative events, including enabling and disabling logging, recorded?
Management
Are the Operating System (OS) and applications, data and database, and logs loaded on separate logical or physical partitions?
Are access rules added, modified, and deleted as business needs change?
Management Practice
Does the training include how to store devices when not in use safely?
Does the training include proper password selection?
Does the training include the approved uses for company devices?
Does the training include the type of information that the devices may store?
Does the training include the type of programs that can be installed?
Is there a process to report lost or stolen devices, and are users made aware of this process during their security training?

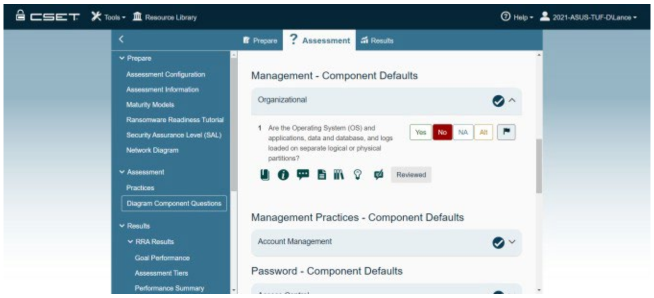
Is wireless security training required of users before being issued a company handheld wireless device?
Are there standardized security configurations for client devices and access points?
Are wireless security configuration implementation and maintenance standardized, automated, and centralized?
Are user and Administrator account permissions/access based on least privilege principles?
Are administrative default accounts, Administrator or root, renamed?
Do frequent and regular manual and automated security testing occur?
Are audits performed regularly as defined by corporate policy for potential security and permission violations?
Are all personal firewalls, those that are hosted on workstations and laptops, centrally administered?

Is an access banner displayed on computers providing notice that unauthorized use of the equipment may result in disciplinary action?
Password
Are passwords not allowed to be reused?
Does the company have and enforce a policy for altering user and administrator passwords at a regular interval?
Does corporate policy support and enforce firm administrator and user passwords?
Are password defaults changed?
Physical Access
Are critical servers (domain controllers, application servers, PBX, video management systems) physically secure from unauthorized access? (i.e., located in a locked room)
Policies and Procedures General
Is anti-malware software installed, running, and updated based on corporate policy?
Does the company have and enforce a policy for backing up firewall configurations?
Does the company have and enforce a policy for locking out inactive administrator sessions?
Does the company have and enforce a policy for locking out inactive user sessions?
Does the company have and enforce a policy for periodically applying security patches?
Are firmware patches reviewed and applied in a timely fashion as defined by the corporate security policy?
Remote Access control

Is remote access restricted to secure means only, such as AD secured, SSH, or 802.1X, and insecure methods such as VNC or telnet prohibited?
Securing Content
Do application errors return a generic message rather than a detailed error?
Are CGI execute permissions restricted to only those folders that require them?
Is wireless access based on a list of hardware addresses (MAC address) that can be registered and tracked?
Securing the Component
If there is no file extension, does the system return a 404 error?
Have the default “out-of- the-box” security settings been reviewed and modified?
Are portable media, such as CD-ROM drives, DVDs, floppy drives, or USBs, disabled or limited for use only by system administrators?
Are all sample applications, toolkits, SDKs, and new virtual directories removed?
Is a robust Uninterruptible Power Supply (UPS) utilized to minimize the impact of a power loss?
Are devices labeled with the company name, address, and phone number if the device is lost?
Securing the Router
Are the device’s incoming packets sourced with invalid addresses disallowed?
Securing the System
Are events logged and alerts issued if typical attack profiles are detected?
Do administration, log transfers, and system updates to and from the device occur using secure protocols, such as HTTPS, SSH, SFTP, SNMPv3, and are all insecure, clear text communications disabled?
Does the device sync system time to an accurate and reliable clock?
System Protection
Are host-based Intrusion Detection Systems (IDSs) used to alert administrators of anomalies?
User Authentication
Does the system utilize an authentication mechanism such as Active Directory, LDAP, or a Kerberos server?
Is Web-based authentication via SSL or TLS only?

3.2 Cyber Security Evaluation Tool

The researchers used this tool to provide a systematic, disciplined, and repeatable approach for evaluating an organization’s security posture.



Management - Component Defaults

Organizational

1 Are the Operating System (OS) and applications, data and database, and logs loaded on separate logical or physical partitions?

Management Practices - Component Defaults

Account Management

Password - Component Defaults

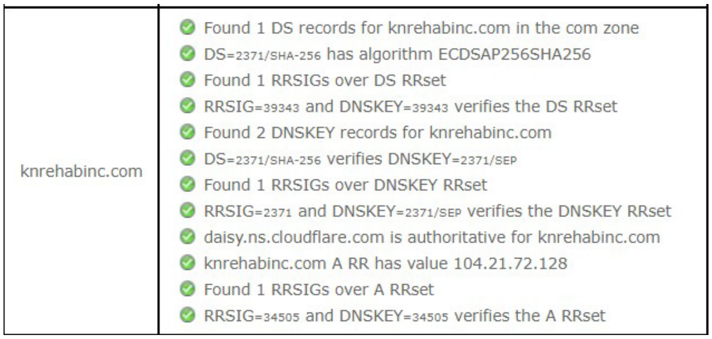
Figure 2. Cyber Security Evaluation Tool

Presented in figure 2, the CSET includes a graphical user interface for diagramming the control system network architecture and classifying network components according to their "criticality." By generating a network architecture diagram, users may identify the organization's cybersecurity zones, key components, and communication conduits. Users may create diagrams by dragging and dropping different system and network components into position. Specific inquiries aid in the identification of each component in more depth.

After that, CSET creates questions based on the network architecture and chosen security requirements. The assessment team determines the most appropriate response to each question based on the organization's current network setup and security policies and procedures. The program analyzes completed responses to the standards' specified criteria and produces a list of recognized best practices and security holes.

Google Admin Toolbox resolves Google Workspace-related problems. Browser info is a client-side debugging tool that runs in the browser. You may search for apparent facts that may affect how people interact with the Internet. User-agent is a program that performs an analysis on the user agent string.

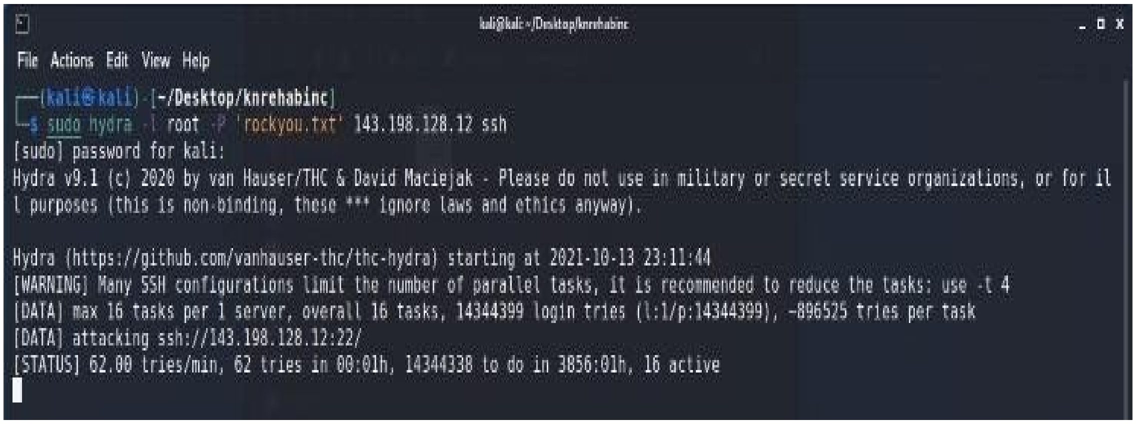
Censys maintains a complete inventory of your Internet assets using their Internet Discovery Algorithm and cloud connections. DNSSEC Analyzer is a tool we use for examining a DNSSEC-enabled domain name's "chain of trust." The program walks you through the DNSSEC validation process for a particular domain name and identifies any issues that are discovered.



knrehabinc.com	✓ Found 1 DS records for knrehabinc.com in the com zone ✓ DS=2371/SHA-256 has algorithm ECDSAP256SHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=39343 and DNSKEY=39343 verifies the DS RRset ✓ Found 2 DNSKEY records for knrehabinc.com ✓ DS=2371/SHA-256 verifies DNSKEY=2371/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=2371 and DNSKEY=2371/SEP verifies the DNSKEY RRset ✓ daisy.ns.cloudflare.com is authoritative for knrehabinc.com ✓ knrehabinc.com A RR has value 104.21.72.128 ✓ Found 1 RRSIGs over A RRset ✓ RRSIG=34505 and DNSKEY=34505 verifies the A RRset

Figure 3. Verisign LABS

As shown in Figure 3, the verisign labs tool analyzes the authentication of domain name systems. In the figure above, the domain name system implemented all safeguards to prevent e-mail and DNS external threats. Hydra, one of the tool used in this study, comes pre-installed with Kali Linux. It is used to brute-force usernames and passwords for various services, including FTP, SSH, telnet, and MS-SQL. Brute-force is a technique that compares particular usernames and passwords to a predefined threshold to ascertain correct credentials.



```
┌──(kali㉿kali)-[~/Desktop/knrehabinc]
└─$ sudo hydra -l root -P 'rockyou.txt' 143.198.128.12 ssh
[sudo] password for kali:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for il
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-13 23:11:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://143.198.128.12:22/
[STATUS] 62.00 tries/min, 62 tries in 00:01h, 14344338 to do in 3856:01h, 16 active
```

Figure 4. Hydra

As shown in Figure 4, the researcher attempted to brute force the organization's web server. SSH keys were not implemented in the server, and the port number was not changed.

While there are services that analyze the HTTP response headers of other websites, Security Headers by Probely include a grading system in the findings. The HTTP response headers analyzed by this site offer significant degrees of security, and it is critical that sites use them. By offering a simple method for assessing them and more information on how to deploy missing headers, we want to increase the use of security-related headers throughout the web.

4. Results and Key Findings

The number of identified warnings and recommendations in the fundamental analysis of the user-defined system is presented in Table 2

Table 2. Analysis of IT Components

Component	Yes	No	N/A
Firewall	28%	26%	46%
Web Server	47%	11%	42%
Handheld Wireless Device	37%	7%	56%
Personal Computer	43%	14%	43%

Upon analysis on the network diagram of the case site in this study. Findings include that the network path identified by the components, NGINX Web Server and Webmaster, connects network segments whose components reside in different zones. A firewall to filter the traffic on this path is recommended to protect the components in one zone from a compromised component in the other zone. The subnet should have an IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) inline to confirm that the firewall configuration, Cloudflare Proxy Server, is correct. That malware has not been able to penetrate past the firewall. The path identified by the components, and NGINX Web Server, appears to connect on one side to an external network. A firewall to filter the traffic to and from the external network is recommended to protect the facility's network. Note that a 'Web' component, 'Vendor' component, or 'Partner' component are all assumed to interface with an external network. In addition, a modem with a single connection is assumed to allow a connection from outside the facility's network.

5. Conclusion & Recommendation

The standards-based security evaluation demonstrates that a concentrated effort to solve the issues highlighted in this study may result in significant security improvements. Most of the issues highlighted need a sophisticated or high-tech remedy and establishing security policies is strongly advised. Adhering to the Cyber Security Evaluation Tool's findings as a guideline for improving cybersecurity is critical for achieving the intended security objective.
For the Google Workspace, Domain Name System, and virtual machine of the case site company to remain secure, they must be reassessed regularly. At the very least, yearly, or promptly after a significant breach, is recommended. We conclude that the security of the. Staffing Agency case site in this study should be enhanced.
Based on our findings, the researchers recommend the following:

To help prevent spoofing and spam with SPF. A DNS record called an SPF TXT record verifies the domain name from which email messages are delivered, so assisting in the prevention of spoofing and phishing. SPF verifies the IP address of the sender against the purported owner of the transmitting domain to validate the origin of email communications (Microsoft 2022).
To increase security for an outgoing e-mail with DKIM. Set up DKIM to shield your domain from spoofing and stop spam filters from flagging your outgoing communications. The From address of an email message is forged in a sort of email assault known as spoofing. A communication that has been faked looks to come from the fake company or domain. DKIM can identify when a message has been altered and when the From: address has been changed without authorization (Google Workspace 2022).
To increase security for forged spam with DMARC. DMARC, or Domain-based Message Authentication, Reporting & Conformance, is an email authentication mechanism that builds on SPF and DKIM, two further email authentication techniques, to determine whether an email message actually comes from the location it claims to have. In addition to email authentication, it also has reporting features, allowing domain owners to look at email authentication data for their own domains. DMARC's primary goal is to stop phishing and email spoofing. In recent years, email phishing has been a significant security concern. According to research, about 50% of cyberattacks target small firms, and over 90% of network breaches begin with a phishing email. A security breach puts a lot of things at risk for a company, including damaged brand reputation, intellectual property theft, immediate cash loss, etc.(Dmarcly 2022)
Set up Cloudflare Origin Certificate to server. Depending on the level of protection required and the amount of configuration you're prepared to do, Cloudflare SSL functions in various modes. Your website will always benefit from HTTPS because traffic to the end user will always be encrypted. However, there are many different ways to set up the traffic between Cloudflare and your origin server (Cloudflare 2022).

References

Bhuyan SS, Kabir U, Escareno JM, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J Med Syst 2020;44: DOI: 10.1007/s10916-019-1507-y

Cloudflare. Dedicated SSL Certificates. Available: https://www.cloudflare.com/ssl/, 2022

Cybersecurity: How can it be Improved in Healthcare? Chicago: University of Illinois. https://healthinformatics.uic.edu/blog/cybersecurity-how- can-it-be-improved-in-health-care/ (July 2020, date last accessed).

Dmarcly. What is DMARC (Domain-based Message Authentication, Reporting & Conformance)?. Available: https://dmarcly.com/blog/what-is-dmarc-domain-based-message-authentication-reporting-and-conformance, 2022

Google Workspace. Help prevent spoofing and spam with DKIM. Available: https://support.google.com/a/answer/174124?hl=en, 2022

Healthcare Information Security: Best Practices for Healthcare. Information Security Institute. https://resources.infosecinstitute.com/catego-ry/healthcare- information-security/is-best-practices-for-healthcare/ (May 2020, date last accessed).

Humayun, M; Jhanjhi, NZ; Alsayat, A.; Ponnusamy, V.; Internet of things and ransomware: Evolution, mitigation, and prevention, Egyptian Informatics Journal, Volume 22, Issue 1, Pages 105-117, 2021, ISSN 1110-8665, DOI: 10.1016/j.eij.2020.05.003.

Hu, H. & Wang, G. Revisiting Email Spoofing Attacks. New York, United States: Department of Computer Science, Cornell University, 2018.

Kour, J., & Ahmed, H., E-mail attacks: Investigation about the vulnerability of the Swedish organizations against e-mail threats, 2020.

Microsoft. How Microsoft 365 uses Sender Policy Framework (SPF) to prevent spoofing. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide, 2022

NCCIC. NCCIC ICS CYBER SECURITY EVALUATION TOOL. Available: https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf,

Newman, R. C. , Cybercrime, identity theft, and fraud. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, 2006- InfoSecCD '06. doi:10.1145/1231047.1231064

Pandemic profiteering: how criminals exploit the COVID-19 crisis. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publications- documents/pandemic-profiteering-how-criminals-exploit- covid-19-crisis (May 2020, date last accessed).

Biography

Dr. Eric Blancaflor is an Associate Professor of Mapua University, Philippines. He earned B.S. in Electronics Engineering from Mapua University, Master's in Engineering major in Computer Engineering in the University of the City of Manila and Doctor of Technology in Technological University of the Philippines. He has published conference papers related to IT systems, network design and security.

Eduardo Jose P. Del Rosario is a graduate of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into Programming, Web Development, Internet of Things, Network and Systems administration.

Kent Andrei Dominique M. Tan is a graduate of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into Programming, Web Development, Internet of Things, Network and Systems administration.

Lance Michael A. Delariarte is a graduate of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into Programming, Web Development, Internet of Things, Network and Systems administration.

Christian Earl A. Santos is a graduate of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into Programming, Web Development, Internet of Things, Network and Systems administration.

David Allan R. Uy is a graduate of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into Programming, Web Development, Internet of Things, Network and Systems administration.