12-2020

RCAP Solutions Breach Management - Case Study

Eugene Adu-Gyamfi
Clark University, eadugyamfi@clarku.edu

Gio Al Muarrawi
Clark University, galmuarrawi@clarku.edu

Kwame Ofori
Clark University, kofori@clarku.edu

RCAP Solutions Breach Management - Case Study

Eugene Adu-Gyamfi

Gio Al Muarrawi

Kwame Ofori

Clark University

Richard Aroian

Table of Contents

Section 1: Method

Companies get hacked every day, and our in-scope company for this case study, RCAP Solution, was not an exception. Security incidents have increased both in volume and range in recent years, and cyber-attacks have become more sophisticated than ever before. There are so many reasons that drive this fact; one is that our infrastructure was not protected efficiently, but also attackers have become more knowledgeable in initiating advanced attacks at a scale. Additionally, the entrance of emerging technologies such as blockchain, machine learning, and the internet of things, added additional complexity to the already complex scene. Cybercriminals are using various attack vectors to target their victims. According to Check Point Cyber Security Report, 27% of all organizations globally were impacted by cyber-attacks that involved mobile devices in 2019 (Check Point Cyber Security Report, 2020).

Many security incidents happened last year, but phishing attacks were one of the significant attacks initiated in 2019. Phishing is not a new attack; however, it is getting more popular with more efficient techniques using spear phishing, which is a more targeted attack. In general, phishing attacks happen more frequently than other types of attacks (Brute force, DDoS, Malware, etc.) because it is easier to initiate and most cost-effective.

Although breaches involved phishing were only 22% of the overall breaches in 2019 (Verizon, 2020), it remains one of the most straightforward attacks to establish. Nowadays, spear-phishing, which targets a specific organization department or employee, is considered one of the most critical phishing types. RCAP Solution Company recently got a security incident of a phishing attack that leads to a security breach. We selected this incident at RCAP solution for our case study because we believe it would help to understand the big picture on how companies, just like RCAP, are handling such incidents, and what checks and balances are in place to prevent, detect, and react to avoid future similar incidents.

Our approach was to understand the risk and controls environment within the RCAP Solutions, but also to deep dive in this particular incident to see how the company handled it from an incident management lifecycle perspective.

For this case study, we used different methods of collecting the information, analyzing the problem, and documenting the results. We mainly relied on quantitative analysis along with qualitative to support the facts. We supported that with deep research in incident management field and looked up best practices to benchmark our results to, such as NIST Cybersecurity Framework (CSF), and NIST Special Publication 800-61 Revision 2. This helped our study by standardizing the approach and provided supplemental tools that benefited our case.

Also, we obtained access to some internal data, information and reports that helped to provide some statistics and facts regarding what happened before, during, and after the phishing attack that occurred at the RCAP Solution.

For security reasons, we redacted all sensitive information to ensure data confidentiality and privacy but at the same time, we made sure integrity in our analysis is guaranteed.

Section 2: Literature Review

The advent of the internet around the world has brought a lot of benefit to people and businesses. Over time, the need has been realized to allow for a lot of devices connect and communicate with each other to make life simpler, a phenomenon known as the internet of things. Thus, has led to more information entrusted to such devices and systems. Personal and sensitive information may be available on such systems and networks, that lack the security measures to protect this information.

Communication systems have become more vulnerable and can be easily attacked by malicious users through social engineering attacks. (Salahdine & Kaabouch, 2019)

(Salahdine & Kaabouch, 2019) describes how humans have become the weakest link in the security chain because of trust. Humans are more likely to trust other humans compared to computers or technologies. Due to this, social engineering attacks have become the biggest threats facing cybersecurity (Foozy et al., 2011). The commonest of this attack by social engineers is the phishing attack. They aim at fraudulently acquiring private and confidential information from intended targets via phone calls or emails. Attackers mislead victims to obtain sensitive and confidential information. Phishing attacks come in several forms: e-mail messages, phone calls, messages via social network amongst others. More than ever, it has become expedient for organizations to inspire a culture of security awareness amongst their employees. (Salahdine & Kaabouch, 2019), proposed several techniques to detect and prevent such attacks which include: encouraging security education and training, increasing social awareness of social-engineering attacks, providing the required tools to detect and avoid these attacks, learning how to keep confidential information safe, reporting any suspected activity to the security service, organizing security orientations for new employees, and advertising attacks’ risks to all employees by forwarding sensitization emails and known fraudulent emails. (Salahdine & Kaabouch, 2019) also realized that most of the social engineer attacks such as phishing are complex and hard to detect because of their human factor, therefore making mitigation necessary. The mitigation technique looks at reducing the impact of the attack on individuals or organizations. It outlines security actions that ought to be implemented in case of an emergency to minimize loss as much as possible. It saves valuable time in responding to an attack and stopping the spread of the attack into the company’s network. Previous studies have often been focused on either the management or the technical point of view. (Foozy et al., 2011)

The focus of our paper is to use the NIST Cybersecurity Framework (CSF), and NIST Special Publication 800-61 Revision 2 as the recognized standardized documentation in addressing phishing-related attacks in an organization by considering all areas prone to vulnerability. The purpose of this NIST guideline is to establish an effective response program with the aim of detecting, analyzing, prioritizing, and handling incidents. (Cichonski et al., 2012)

Section 3: Background Information

As technology remain a crucial part of organizational workflows, each company needs to prioritize the security of its information and actively work to ensure proper security measures are implemented in the right circumstances. Technology today accounts for some of the most intriguing complicated systems and has become one of the main enablers of the digital transformation of the world. In this incident analysis, we will be assessing the implemented security measures that were nonexistent or existent and how they could have played a role in the outcome of the initial account breach. When it comes to technical issues in Information technology, the company always benefits if issues and concerns are addressed before they occur rather than reacting to them after they have occurred. This incident analysis is focused on the RCAP email breach that took place on September 1st, 2020 at 9:00 am. The user’s account credential was then used to send out massive phishing emails to many external users. As much as this could have been resolved with implementing an incidence response policy, mail account alerts, incident detection and real-time analysis. In the issue of a phishing attack, phishing attackers try to gain access to the organization’s workstations. In compromising the user's account, the attackers can gain access to vital and sensitive information in the organization such as intellectual property, money, and client identity information (social security numbers and drivers licenses). Often, many attacks can be categorized as phishing, but the primary means of attack is usually any email-based attack that has the goal of luring a response from the email recipient. As we discuss the impact of this type of security breach, we learn to understand that phishing remains a pending issue and Often, phishing emails are carefully crafted and targeted to specific recipients and given the number and intensity of data breaches witnessed over the last several years. Due to the nature of the information and its security sensitivity, we will not be releasing the proceeds from our finding to the general public but we will have detailed conversations with our points of contact from the organization we are doing this incidence investigation for. Since all our proceeds and findings will be discussed with the company representatives we are working with, the target audience for this case study will be the people listed in the stakeholder's documentation that was included with the program charter. Cyber attackers often compromise personal and business data, and it remains essential for organizations to be able to respond quickly and effectively when these types of security breaches occur. One of the benefits of evaluating this data breach is that we can use the information gathered to minimize loss, theft and lower the disruption of services caused by the breach incident in the organization.

Section 4: About the Organization

RCAP Solutions is a nonprofit organization that is aimed at assisting families to gain access to affordable housing and help to decrease the homelessness rise in the city of Worcester. Established in the year 1969, RCAP solution continues to provide help to individuals, families, communities, and small business owners with a varying range of housing and other beneficial services for the past 50 years. The organization started in a small office in Winchendon and continued to grow. As years passed, they established a headquarters in Gardner, Ma and attained secondary office location in Worcester, MA. Expansion and progress propelled the organization further and they attained various remote sites that ranged from Athol, Bolton, Groton, northbridge, webster, Hubbardston and many more. RCAP Solutions seeks to be the first choice of small and rural communities for the kind of planning, consulting, and direct services that in large cities would be provided by dozens of different departments and private entities. Some of the key services rendered by RCAP solutions include technical assistance to address economic vitality for communities and individuals of which RCAP Solutions helps rural communities and people to build and maintain economic vitality. They assist rural communities and people today, as they plan for tomorrow. By understanding demographic predictions as well as economic indicators, they help communities to envision and address potentials needs that can erupt in the next 5 or 10 years as ageing population demands, and requests will dictate. Services offered in the past include Drinking Water and Wastewater Evaluation and Upgrade, Customized Income Surveys, Community "Visioning" addressing the ways towns can prepare for future, demographic change evaluation, Grant Writing Assistance, Other Environmental and Infrastructure Services, Water and Wastewater Trainings (See Table 2 in appendix for Organizational Chart).

Additionally, RCAP Solutions includes support to increase individual self-sufficiency. Services focus on counselling and resource referral services assisting individuals in the areas of housing, such as apartments or affordable homes, education and training and job readiness as well as a range of workshops for individuals to understand and address changes in the workplace and community of today and tomorrow. Services offered in this area include housing issues, apartment locations, first time home buyer services, domestic violence transitions, multi-lingual counselling and support, education and training: homebuyer workshops, water and wastewater training, and more, job training (i.e., future town water technicians, building inspector trainings, and others), various other self-sufficiency strategies.

Section 5: The Challenge

As an organization that deals with client information and sensitive user data, RCAP solutions remains a primary target for hackers and cybercriminals. There are potentially millions of ways the organization could be targeted and having adequate system logging and computer security software is necessary to ensure user information is protected. Backing these systems up with instituted organizational logging standards and security software standards allows the system to be more effective. Adequately prioritizing the handling of cybersecurity events and incidents when they occur allows the organization to identify situations that are of greater severity and requiring more attention.

Currently, RCAP lacks a formal, focused and coordinated approach to respond to security incidents. This lack of plan means that incidents lack a road map for deriving solutions for the incidents and task that arise in the security department. In such organizational plans, there is a need for a proper procedure and process for handling incidents that align with the designated company codes. RCAP also lacks an incident response team that primarily investigates and avail themselves for the organizational needs when an incident occurs.

To obtain a holistic view of what exactly happened, we utilized the tools provided in the NIST SP 800.61 revision 2 (see Table 1. Incident Handling Checklist in the appendix section). Upon further investigation with the security administrator, before the incident, the organizations lacked adequate incident handling communication and facilities system. There is no established issue tracking system that tracks incident information and status. They currently utilize Off-The-Shelf (OTS) ticketing system; however, this system does not integrate any incident handling procedures or protocols. Issue tracking and adequate logging should be enabled for this system to ensure that the proper contacts and personals are alerted should a security incident occur, but the current infrastructure lacks these capacities. From a hardware system, the need for laptops and packet sniffers and protocol analyzers along with evidence gathering hardware for needed for once an issue occurs are currently absent in this environment. All these technologies are supposed to serve as safe guards for when a security incident occurs. If these systems would have already been in place before an incident occurs it would make it easier to detect the incident. These systems primary goal is to proactively help identifying and detecting if a cybersecurity incident takes place. Ideally, RCAP Solutions needed to build an incident response team for the organizations as single point of action to run and execute the incident handling through the incident lifecycle management. As an incident response team, they need to create jump kits which will contain the tools and resources they will need to properly address an incident once it occurs.

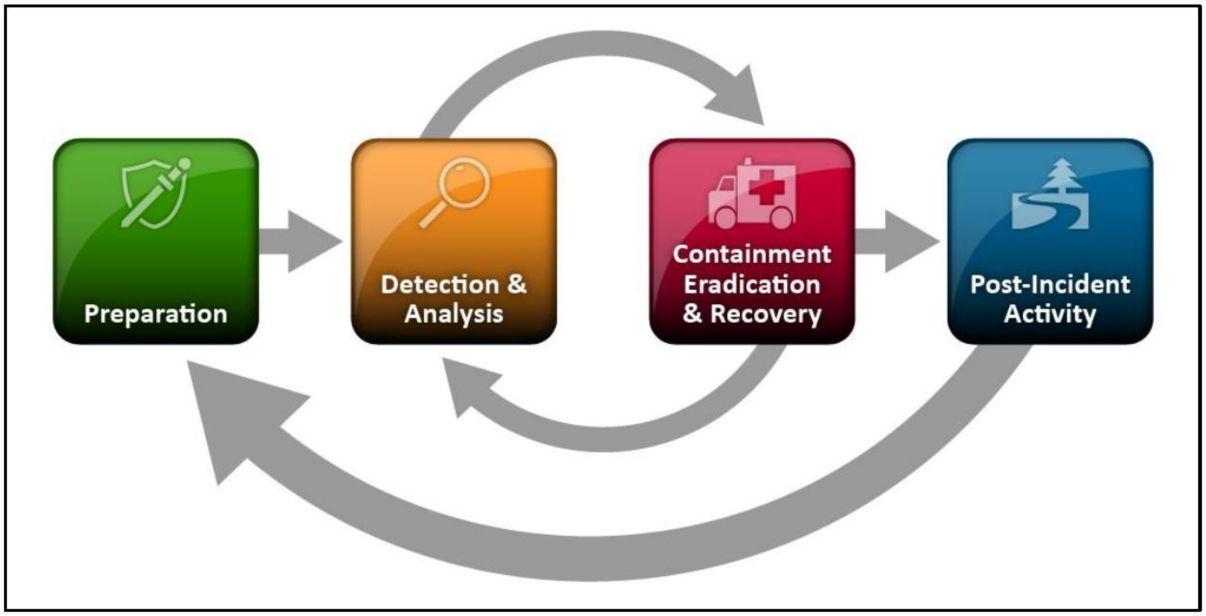
As for the RCAP organization, they could not constantly be dealing with security incidents and breeches as this lower's productivity time and efficiency of the entire organization. Protecting the business processes and sensitive documentation is essential to the organization and having insufficient security controls causes higher volumes of security incidents and this, in the long run, causes more damage and prolonged periods of data and service unavailability. To access the efficiency of security policies, system and procedures, risk assessments must be held. This periodic risk assessment should address systems and applications regarding potential applicable threats and organization-specific threats. RCAP Solutions has a large client base and they deal with client sensitive information. Since this data must be protected, all potential risks against that system should be assessed and identified. This could've helped the RCAP Solutions to understand what needs to be protected and how they can efficiently secure and protect their data resources. Under satisfactory conditions, each risk that the organization exposes must be prioritized so that it can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. As the organization utilize risk assessments to address acceptable security policies and systems, the organization need to prioritize user awareness and training. Apparently, the lack of user training and awareness put the entire organization at risk because the users are essential, the first level of defense for most malicious attacks, but at the same time are the weakest point in the security chain, still. In this particular security breach incident at RCAP solutions, had users that lacked email and phishing awareness. Organizations must ensure that users are made aware of company policies and procedures regarding the appropriate use of networks, systems, and applications. Applicable lessons that are learned from previous breeches an incident is to be disclosed to other users in information ways that can allow them to learn from the experience too. Once policies and procedures are covered, there is a need for malware prevention software that can halt the rapid spread of malware in the organization. These malware prevention and protection configurations can be deployed at the host level, the server level and even the application level. In RCAP's incident, there was an email proxy server that was dedicated to email filtering and spam handling but the configurated was only limited to inbound email traffic. This left the outbound mail vulnerable. Hence, once the phishing attack makes it through, there was no way to catch it as it was duplicating itself and resending itself in the organization. For more details on the RCAP Solutions security breach report, kindly refer to Report 1 in the Appendix section.

From a technical standpoint, the root cause of the breach was a lack of adequate user training in the organization. The attack started through a phishing email, getting past the email proxy server. Just like any other email attack, the email contained an attachment link that redirected to a private server where user credential and passwords are stored for access later by the perpetrators. We believe as much as this attack was an email attack, there was a great deal of impersonation that took place in the incident. Once a user clicked on the link and was sent to the non-secure website, user credentials that were entered get stored and the next phase of the attack begins. Information and credentials collected are then used improperly to send out more malicious emails. There were no adequate security systems in the organization that could have efficiently mitigated the issue. Although this was not the first phishing email attempt in the organization, the damage to the infrastructure was enormous and productivity was greatly affected by the breach. This breach originated from an unforeseen source and remains a product of various malicious external forces.

Section 6: The Solution

From a solutions standpoint, we discovered that RCAP solutions ultimately lacked incident management framework. Down the line the company also lacked both precursors and indicators in their Security infrastructure. A precursor is a sign that foreshadows that a potential incident may occur. Since this incident went undiscovered, deep, specialized technical knowledge and the extensive experience was necessary to properly and adequately analysis all data related to this incident.

The framework would help the company to put a perspective around handling any security incident throughout its lifecycle (prior, during, and after). The below graph illustrated



Source: NIST.SP.800-61r2, p21

Preparation is key phase to start with beside establishing incident capabilities so that the organization is ready, but more importantly preventing incident via ensuring all technology layers (systems, network, applications, and database) are sufficiently secured.

Technology failed as a security resource for RCAP. It failed to detect any triggers about the breach. The organization found out about the incidental breach when they were alerted by phone calls and emails from receivers who had received the duplicated copy of the original malicious phishing email. This failure of our technological infrastructure meant that we had to perform a manual investigation to be able to account for the damages that had occurred. Utilizing system logs to access or identify the breach was an impossible feat because the incident transpired between the application layer of the infrastructure and logs monitored on this level are specific to programs running. This would have meant that looking through workstation and Operating system logs would have been useless, but instead, RCAP was able to utilize the logs from the user sign In times while combining the events in the email proxy to provide accurate time stamps of the incidents. The connection between the sign-in times and geographical location along with made it easy to discover the breach in the system. From the analysis, we discovered that they were only one compromised email but duplicates of the initial phishing email had already been sent out to both internal and external users. At this juncture, the team was able to easily detect malicious activities in the email. Unlike the usual conventional approach, the RCAP team decided to investigate the outbound proxy setting for the organization since many emails were sent out after the initial email was compromised. Upon extensive research into the proxy settings, we discovered the security baseline was not hardened to enable outbound email monitoring. Granted this would not have prevented the initial phishing email, it instead allowed us to perform a thorough investigation. After the user clicked on the phishing email with the bad link, they were renavigated to an unsecured site where they were then asked to sign-in to their Microsoft account. Credentials that are entered are cached into notepad documentation and misused by the perpetrator to access unauthorized locations. The credentials stolen from this organization compromise the confidentiality, integrity, and availability of the organization. Per further analysis, the compromised account had access to some financial documentation and programmatic sensitive data that were deemed to be rated as a medium risk. As an organization, RCAP solutions had preventative controls that failed but the team had detective controls that were already implemented.

These controls enabled RCAP to gather information about the incident utilizing the system and email logs. From a process standpoint, RCAP lacked an incident response team and there was no security standard threshold to be upheld. From a people perspective, the organization lacked adequate user training. Employees were not required to partake in internet security training or other interactive learning activities; hence, they were not able to assist in mitigating the attack due to a lack of cyber knowledge and understanding. As an organization, there is a need to efficiently profile RCAP's networks and systems. Adequate documentation must be provided and maintained in the organization. The knowledge base of information that serves as quick references during an incident should be kept and updated by the organization’s security admins. Documentation of the environment needs to include a variety of information, along with explanations of the significance and validity of precursors and indicators. These knowledge base of information can either be text documents, diagrams, spreadsheets, or relatively simple databases that can provide adequate, flexible, and searchable resources for the environment to utilize. Furthermore, the whole control environment can be mapped out to the NIST CSF and an evergreen process can be established to ensure control design and operational effectiveness are in place.

Once the team was alerted to the breach, the RCAP technical team began work immediately on the incident. They began by securing the compromised account and isolating it to a sandbox environment for further investigation. The sandbox isolation is a means of containing the breach before the incident overwhelms resources and increase the damage it has already caused. Since the attack transpired using the user's email account, the RCAP email account that was compromised to allow the perpetrators' access was blocked from sign in and investigative tests began on the account.

A ticket for the data breach was created to serve as a centralized space to consolidate all the evidence and research that is collected. To protect the confidentiality of the information collected, the data was safeguarded and restricted as it contained a lot of explicit user information and account details about the compromised employee account. The IT Team collected identification information about the account login and this information included locations, serial numbers, IP address, and programs used to access the account. There were also a lot of system-related information like Mac addresses and other sensitive information the following outlines were made in the ticketing system to help collect and centralized the evidence data.

a) Status of the Ticket: This was updated every week and detailed the current status of the ticket.

b) Incident Summary: This section allowed the Technical team to detail out their perception and explanation of the incident that took place in the organization.

c) Files / Resources: This section provided a list of all the information and evidence gathered by the team during the incident.

d) Notes/ Other: In this section, the team detailed and logged all they had done in relation to the ticket.

The breach incident was treated with a high sense of urgency because business at RCAP Solutions was greatly affected by it. The malicious email was being replicated and sent to all the users in the address book, so resolutions had to be implemented quickly. Another factor was that the compromised account belonged to a manager and that account had access to other financial and programmatic resources, so it was a top priority to secure the account and mitigate the ongoing issue.

Since the account belonged to a user with elevated privileges, RCAP included the VP of operations along with the IT representatives. The VP was tasked with communicating the status of the issue with the whole organizational and keeping them updated while the IT team worked on resolving the incident and getting the user fully working again all while mitigating the damage that has occurred. The VP of operation also created a report that was presented to the board of directors of the company. This report detailed efforts after the breach attack and what the organization was doing differently to reinforce better security in the environment. To address legal proceedings, the VP had to include all compromised systems and how they had been preserved in the past.

Since this was a breach through a phishing email, it was difficult to come up with a comprehensive solution that was fit for the attack, but the IT team was able to develop some long and short term projects that would secure the infrastructure while providing more security and resistance toward a similar attack. As an organization, RCAP knew that to fully secure its environment, it had to harden the provisioned system baselines configurations, improve preventative controls, and potentially implement an effective detection control system. Immediately after the incident, short term solutions had to be readily available. The RCAP IT team created a sandbox environment, block the IP of the perpetrator, reset the account of the compromised employee, and monitored the activity on the account. For long term permanent solutions and Implementations, we aimed to enhance and increase preventive control and measure in the environment. We contacted Microsoft and purchased Microsoft advance protection 1 & 2. This is a software tool that gives us access into a portal to configure security measures and protocols, including modifying spamming and phishing sensitivity settings in the system. We also aimed to address security baselines standards by redesigning new security baselines for existing proxy servers and a potential modification of firewall rules and setting to allow less junk traffic in the organization. Also, we aim to use the NIIST SP 800-61r2 as a guide and assessment checklist to help us build a disaster recovery plan for the organization. The timeline for these recommended solutions would take from few months to several years depending on the RCAP Solutions resources and budget as well as the senior management decision to replace numerous legacy systems given the cost benefit analysis of future breaches versus the amount of investment required to adapt a new framework, redesign processes and implement addition security controls in the environment.

Section 7: Conclusion

The existing IT infrastructure of RCAP did not provide the adequate defense needed to detect, protect, mitigate cyber threats that target the organization. This leads them exposed to the security breach that occurred through the phishing email. In this security breach, the attacker sent an email that included a link to a login page. Here, the attacker created a login like the one belonging to Microsoft. The page asked for a username and password and after the first entry, it re-navigated to the actual Microsoft sign-in page so the user would just try their credential again a d would be able to log in. This was the cause for the RCAP employee and upon entering the credentials, the attack got access to the internal network, so he sent an email blast from the compromised account to all global contact list in the organization. In this email, was encapsulate a different version of the phishing message contains the same malicious link. The email was sent out to 5086 email address and although 840 were left undeliverable, the remaining 4246 was delivered to the specified email address. The incident left the organization crippled for about 3 days and the technical team investigated and resolved all the issues that arose.

To implement adequate security measures against threats and breeches, there is a deep need for one to understand the assets belonging to RCAP. We will be using the NIST CSF Framework to explain and discuss the cybersecurity risk to the Organization and try to address the discrepancies in their policies and business approach in managing those vulnerabilities. The first function we will address is Identify. In the identify stage, organizations are to develop a comprehensive understanding of their cybersecurity risk accessing systems, data, people, and capabilities. In the Identify function of the cybersecurity framework forms the baseline for system expectations and organizational accountability because it outlines the need for policies that account for the needs and vulnerabilities of the organization. In the cause of RCAP solutions, they lacked a risk management strategy, or an awareness of what systems need to be protected. To counteract this, RCAP must provide a comprehensive business plan that addresses governance, risk management, risk assessment and a thorough evaluation of their business environment.

The next core function of the framework that RCAP must address was providing adequate protection for all the organizational assets deemed necessary to protect. This is very important because it allowed the organization to limit and contain the impact of a potential cybersecurity event. This means that instead of the system sending 8246 emails, it would have blocked the sender and moved that email to the quarantined list until approval from a systems administrator. protective technology, maintenance, identity management and access control.

The source of the breach was not identified and detected until RCAP received a call from the sender of the original email. This not only slowed down the reaction time to the cyber threat but prevented the IT team from mitigating the risk promptly. Detect functions allow early response times to incidents and cyber breaches. Examples of outcome categories expressed by this function include monitoring anomalies and events, continuous security monitoring and adequate detection. The RCAP environment has alert logic management console currently but this device is an intrusion detection system that is focused on delivering logs and identifying anomalies in the network on the packet level of the organization. It is primed for identifying brute forces attacks and incidents that involve fluctuations in network traffic but highly inefficient in detecting application-based attacks. The phishing attack as designed is structured within the email application and the web browsers. Packet monitoring system and intrusion detection devices would not recognize this attack. Adequate email proxy settings could have filtered out the phishing attack.

Once the attack has been detected, the next actionable step is to respond to the impending threat. The respond function is focused on the steps and actions taken help mitigate, contain, and limit the impact of a potential cybersecurity incident. In our case at RCAP, the response was highly inefficient as the scope of the attack and full impact was not adequately communicated. To effectively respond to a respond and mitigate a security incident, the Organization needs to have a thorough response plan, adequate incident analysis and communication process and finally, means to mitigate and improve the organizational environment. The documented response implemented in the RCAP incident is listed below.

Reset the Users account – This response was intended to release the account back to its primary owner. It deauthorized the signed-in account and reset the password of the Microsoft account.

Disabled Email Forwarding and outlook Inbox rules: This rule was intended to remove account configurations that shared email account with other listed email addresses.

The recover function is the final phase of the framework. This phase requires organizations to develop and implement the appropriate activities, needed to maintain plans for resilience and to restore any capabilities or services that were impaired due to a security incident. The recovery function is highly important because organizations cannot develop a fault-proof system and hackers are constantly evolving as solutionist and technologies keep falling further behind. This means that having a comprehensive recovery plan is essential for business continuity. Downtime related to cyber incidents can be reduced greatly if adequate recovery plans and improvements were made. The primary goal of the recover function is to restore the compromised environment into normal operational conditions in as little time as possible. Recovery phase in RCAP's incident was very minimal as no files or server data was compromised.

References:

Barrett, M. (2018). Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25.

Check Point Research. (2019). *Cyber Attack Trends: 2019 Mid-Year Report*. 24. https://research.checkpoint.com/cyber-attack-trends-2019-mid-year-report/

Check Point Research. (2020). SECURITY. *Cyber Security Report 2020*.

Cichonski, P. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, *800–61*, 79. http://dx.doi.org/10.6028/NIST.SP.800-61r2%5Cnhttp://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Foozy, C., Ahmad, R., & Abdollah, M. (2011). Generic Taxonomy of Social Engineering Attack. *Malaysian Technical Universities International Conference on Engineering Technology MUiCET 2011 (2011)*, *MUiCET*, 527–533. http://ftmk.utem.edu.my/zaki/VolumeII/PENULISAN DAN PENERBITAN/4.1/Antarabangsa/Prosiding/4.1.9b/muceit2011cikferesa.pdf

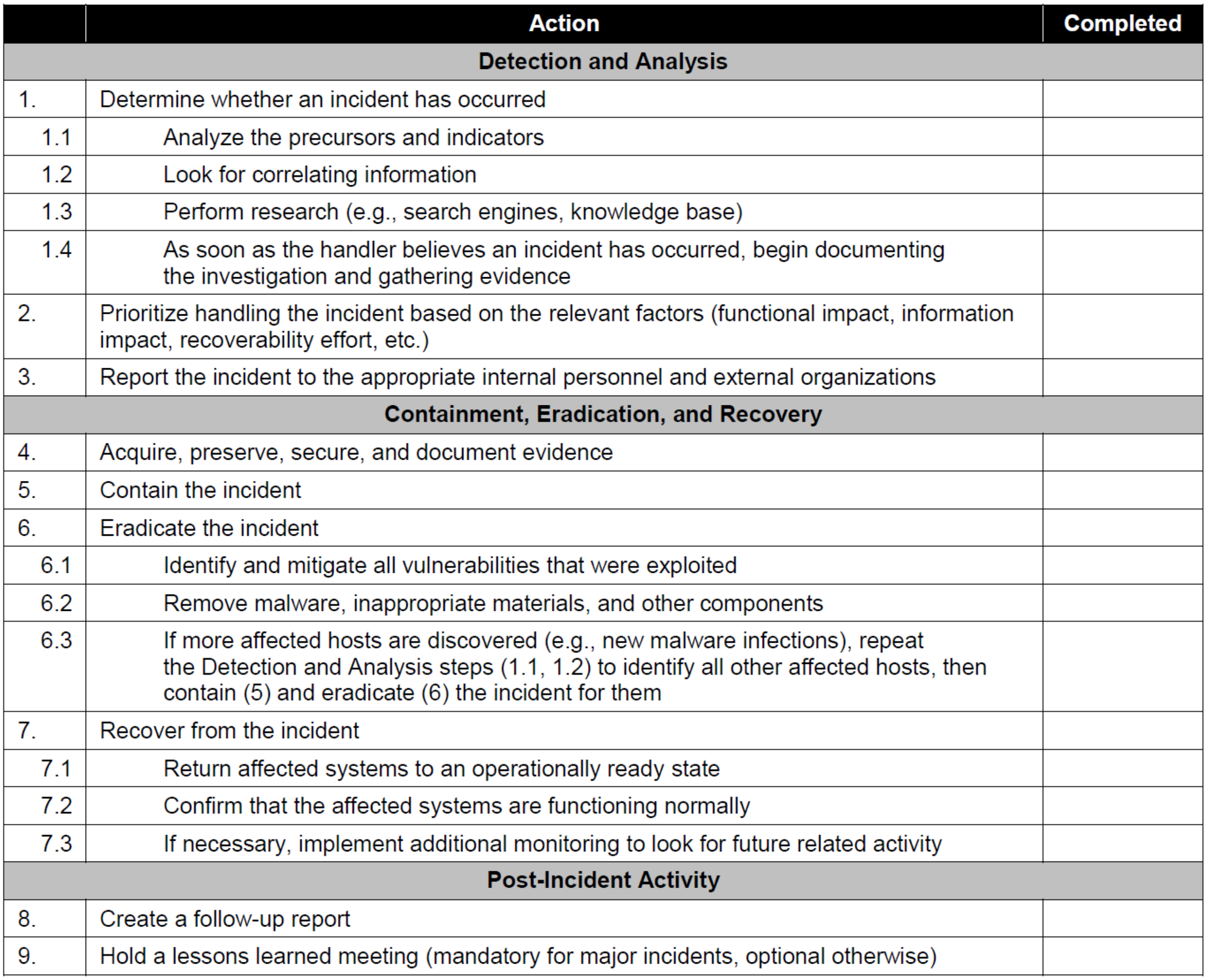
Prevention, T., Ngtx, S., Appliance, R., William, A., Freeman, D., & Williams, J. (2017). *Check Point Software Technologies 15600 Next Generation*. 1–56.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/FI11040089

Nathan, A. J., & Scobell, A. (2020). 2020Data Breach Investigations Report. *Verizon*. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf%0Ahttp://bfy.tw/HJvH

Appendix:

Table 1. Incident Handling Checklist



	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Report 1. RCAP Email Phishing Breach

“

On September 1st , 2020 at 9:00 am , We documented the first case of the Breech.

<u>Application Used by the User</u>

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 OPR/70.0.3728.119

<u>Application Accessed :</u>

- Office 365 Exchange Online,
Office365 Shell WCSS-Client
Skype Web Experience On Office 365

Location

Atlanta, Georgia, US

IP address

66.115.181.78

Again, On September 2nd, 2020 at 9:47 am, We documented another sign into the compromised account.

Application Used by the User

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 OPR/70.0.3728.119

Application Accessed:

Office 365 Exchange Online,
Office365 Shell WCSS-Client
Skype Web Experience on Office 365
Office 365 Exchange Online

Location

Lagos, Lagos, NG

IP address

154.120.94.233

On the Same day, we documented another sign In into the Account

Time: 9/2/2020, 10:19:13 AM

Application Accessed:

Microsoft Office/16.0 (Windows NT 6.3; Microsoft Outlook 16.0.12527; Pro)
Microsoft Azure Signup Portal

Location: Washington, Virginia, US
IP address: 20.185.70.168
On the Same day, we documented another sign In into the Account

Time: 9/2/2020, 11:17:00 AM

Application Accessed:

Microsoft Office/16.0 (Windows NT 6.3; Microsoft Outlook 16.0.12527; Pro)
Microsoft Azure Signup Portal
Chrome Mobile iOS 84.0.4147

Location: Cromwell, Connecticut, US
IP address: 174.242.146.59

Effects

Attackers Logged into Users O365 Account using web password access and Created a Mail rule and also sent out messages.

– 5086 Compromised emails Sent

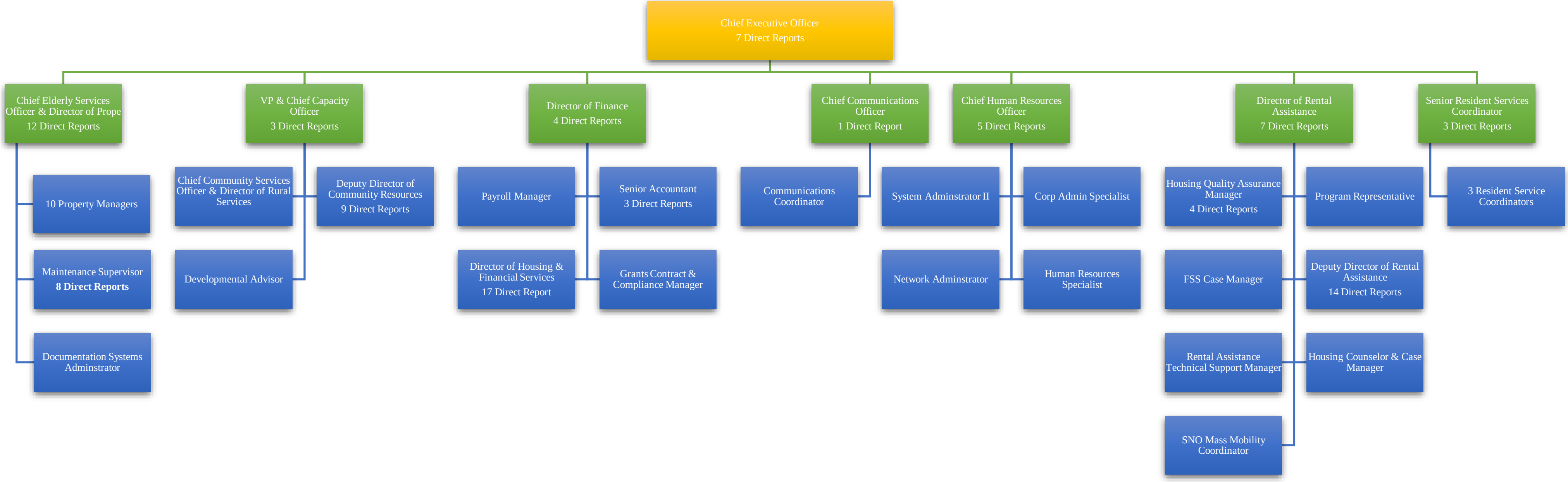
- **840 Undelivered Emails**
- **No Files Accessed on SharePoint**
- **Rule Made in Outlook Web to Delete New Incoming Emails**

Actions Taken to Address Account Compromise

- **Reset the user's password**
- **Checked for Email forwarding**
- **Disabled Outlook Inbox Rule**

“

Table 2. Organization Chart – RCAP Solutions


Chief Executive Officer
7 Direct Reports
Chief Elderly Services Officer & Director of Prope
12 Direct Reports
10 Property Managers
Maintenance Supervisor
8 Direct Reports
Documentation Systems Adminstrator
VP & Chief Capacity Officer
3 Direct Reports
Chief Community Services Officer & Director of Rural Services
Deputy Director of Community Resources
9 Direct Reports
Developmental Advisor
Director of Finance
4 Direct Reports
Payroll Manager
Senior Accountant
3 Direct Reports
Director of Housing & Financial Services
17 Direct Report
Grants Contract & Compliance Manager
Chief Communications Officer
1 Direct Report
Communications Coordinator
Chief Human Resources Officer
5 Direct Reports
System Adminstrator II
Corp Admin Specialist
Network Adminstrator
Human Resources Specialist
Director of Rental Assistance
7 Direct Reports
Housing Quality Assurance Manager
4 Direct Reports
Program Representative
FSS Case Manager
Deputy Director of Rental Assistance
14 Direct Reports
Rental Assistance Technical Support Manager
Housing Counselor & Case Manager
SNO Mass Mobility Coordinator
Senior Resident Services Coordinator
3 Direct Reports
3 Resident Service Coordinators