Incident Response in a Security Operation Center

Josh Higgason

Incident Response in a Security Operation Center

GIAC (GCIH) Gold Certification

Author: Josh Higgason, jhiggason@gmail.com
Advisor: Hamed Khiabani, Ph.D.
Accepted: August 22nd 2020

Abstract

Cybercrime dates back to the late 1700s and remains a threat today. By observing current threats, such as phishing and data compromise, a better understanding may be gained regarding cyber campaigns and threat actors. Consequently, efforts must be made to prevent the continuous siphoning of millions of dollars from the economic system caused by cybercrime. Because the highly skilled personnel working with Incident Response in a Security Operation Center face many challenges, teamwork is essential to overcome the threats associated with cybercrime. Additional factors, such as working across multiple time zones with varying time shifts, personality differences, and unique technical skill levels and abilities, affect the ability to work as a team. Working through these differences brings cohesion and strength to the team. The security operations center learns to accomplish more with the time and resources at their disposal. To thwart cybercrime, the personnel in the Security Operations Center must address current issues, devise innovative plans, and adopt a new perspective to overcome the complicated problems they encounter.

1. Introduction – Cybercrime History

Nearly 200 years ago, the first Cyber Security attack happened. According to The Economist in the 1790s, the French erected the first data network. This network was a powered telegraph system, which was based on connected towers. The system's arms moved in various formations and aligned with different letters and numbers. With this new system, memos could be communicated within minutes in France. Then, in 1834, two wise bankers, Joseph and Francois Blanc, figured out a way to profit from this design. They bribed the telegraph operators to make intentional errors in the messages. Another co-conspirator viewed the errors and shared their findings with the Blancs. A couple of years later, authorities discovered their unethical dealings, and they went to trial. Because no law existed in the books about data network abuse, the Blancs were not convicted (Standage, 2017).

In 1955, David Condon played his "Davy Crockett Cat and Canary Bird Call Flute" into his phone to initially test the theory about how a phone system worked. Because the phone system recognized this familiar whistling sound, it linked Condon to a phone operator. Now, Condon could make phone calls without costing him anything. After his findings were unintentionally shared, others began using this method. The fraudulent use of phone service became widespread. Those individuals participating in this activity were known by the coined name "phone phreaks" (Oliver, 2018).

In 1982, during the Cold War, the Central Intelligence Agency (CIA) devised a way to detonate the Siberian Gas pipeline. This unique plan used no missiles or explosives. The CIA injected code into the gas pipeline's system known by the name "logic bomb." The code was a Trojan horse, a piece of malware designed to deceive users of its real intent. This Trojan horse was rooted in equipment that was bought "by the Soviet Union from a company in Canada." The explosion "was the 'most monumental non-nuclear explosion ever," and the fire could be seen from space. Since the pipeline traveled through a remote area in Siberia, no casualties were reported." This incident had been seen around the world. The world could now visualize the cost and impact of manipulated computer code (The 10 Costliest, 2015).

As seen in the above examples in history, there has been a pattern developing. These patterns will continue over the years and become even more sophisticated.

Josh Higgason, jhiggason@gmail.com

2. Examples of Current-Day Threats

2.1. Phishing

With an increasing number of employees working from home, cybercriminals make a more significant effort to capitalize on their activity. Credential phishing sites crop up daily and attempt to trick their next victim. Fake login pages for popular companies such as Microsoft, WebEx, Zoom, Adobe, and FedEx are created daily. Trend Micro cites more than a 35% increase in "credential phishing attempts involving unknown phishing links from 2018 to 2019." These phishing sites are established with the hopes of circumventing security's detection. Or, better yet, many unsuspecting victims enter their credentials before the site is flagged as malicious (Pajares, 2020).

Email is still another common method by which phishing occurs. Often, people click on URLs sent via email without first validating the source. The link might be deceptive and go to a different site. One reliable way to review an email is to check for grammatical or spelling errors. Popular companies double and triple-check their publications and websites for these simple mistakes. Finally, the received email often leads the reader to believe there is a sense of urgency. For example, ACTION REQUIRED, CHANGE NOW, or ACCOUNT SUSPENDED highlight these emails and prompt the user to act quickly. These action requests attempt to scare the user or make them believe something terrible is going to happen if they fail to follow the instructions. Users must understand the importance of not sharing personal, sensitive information online.

2.2. DDoS

A few years ago, several distributed denial of service (DDoS) attacks were documented by targeted online game systems such as Sony's PlayStation Network and Microsoft's Xbox. A DDoS attack interrupts the ordinary traffic of a targeted server or network. The attack engulfs the systems with an extreme amount of traffic, so the sites become unavailable for legitimate use. These documented attacks occurred during the holiday season, but the hacker was caught. The FBI worked with other law enforcement agencies and detained the domain that was being used for DDoS services. This Christmas time attack attracted the interest of other hacker groups. These groups started a trend of launching DDoS attacks each year during the Christmas season. The 2011 Sony PlayStation incident cost the company an estimated $171 million. This cash loss was huge, considering it was for something that was done "to spoil everyone's holiday." The

originator of this DDoS was a man from Utah who received a 27-month prison sentence and was ordered to pay restitution. However, the amount of restitution was nowhere near what it cost Sony (Cimpanu, 2019).

2.3. Data Compromise

Data compromise refers to gaining financial or individual information through phishing or malware. A common example is the Business Email Compromise (BEC). Of the over 400,000 reports that the FBI received in 2019, losses exceeded $3 billion. Of that $3 billion, BEC type crimes account for approximately one half. Generally, this popular type of attack is easily accomplished and does not necessitate complex coding skills. This attack requires a cyber con artist to compromise a valid business email account. Afterward, an email message is composed and sent to that same company. Within the email, the actor attempts to trick the email recipient into transferring money to the actor's account.

3. Cyber Campaigns and Threat Actors

3.1. Qakbot

Qakbot is a very sophisticated banking trojan that does reconnaissance on the host, steals credentials, and covers its tracks. This clever trojan also checks to see if a virtualization environment exists. Some examples include running process names through a blacklist and reviewing registry entries. Another characteristic is the presence of a signed, valid certificate. With all these tools and resources of just one trojan, what's next? To lessen the odds of falling prey to this trojan beast, companies must require employees to maintain strong passwords and train all employees to remain mindful of the threat.

3.2. Malicious Campaigns

According to Trend Micro, COVID-19 related threats include "email spam, BEC, malware, ransomware, and malicious domains." As new hot topics and occasions arise, threat actors are triggered to take advantage of these new social engineering opportunities. For example, Trend Micro has seen over 900,000 spam messages related to COVID-19, over 700 malware related detections, and over 40,000 malicious URLs. With most of the world "sheltering in place" during this pandemic, threat actors leverage any means necessary to profit. Another

example seen on social media is a message saying, “Get 2 Months of Netflix Premium Free anywhere in the world for 60 days. *Get it now Here” (Developing Story: COVID-19, 2020).

4. Cyber Breaches

A few years ago, a data breach might have affected one or two million people. Now, breaches are becoming more frequent and impact hundreds of millions, perhaps even billions of people.

A couple of examples include Equifax, which is one of the most prestigious credit bureaus. In July 2017, a data breach occurred with Equifax that affected over 140 million consumers. The leaked sensitive information included social security numbers, birth dates, and addresses. The application vulnerability of a website was cited as the cause. Some causes of the incident that were identified include the lack of proper Equifax network segmentation, a failed patching process, and the failure to renew a public key certificate. Once an attacker gains access and is inside the network, it is easier to move around. Checks and balances should have been implemented to ensure that the vulnerable systems were patched. By failing to renew their public key certificate, encrypted data exited the company without inspection.

The last example of cyber breaches is with the search engine Yahoo. In September 2016, Yahoo announced that in 2014 attackers had compromised names, email addresses, and birth dates for about 500 million users. Again, in December 2016, they discovered another breach had occurred in 2013. In total, it was estimated that 3 billion accounts were affected. It was also believed that these were state-sponsored actors, but it was not disclosed which government entity was involved (Swinhoe, 2020).

5. Security Operation Center at Work

Within a Security Operations Center (SOC), a few well-defined roles exist. The first-tier team does triage analysis. This team is responsible for intaking many events and alerts. They determine the relevance and urgency of the alert. If it is deemed urgent, the team assigns it according to the level of attention the event requires. A ticket is created for the event, and the second-tier security analyst team works to determine a root cause.

The second-tier team can remain calm under pressure and are curious individuals by nature. This team reviews tickets created by first-tier personnel, assesses any indicator of compromise (IOCs), tracks down affected assets and determines the scope of the threat.

The next tier includes analysts who look for ways to find threats. These threats may have found their way inside. This group of professionals recommends ways to improve current security tools.

The final tier is the SOC Manager. This individual supervises the entire team of professionals. To ensure that the team remains well-trained and up to date, the SOC Manager finds new talents, coordinates training, and manages escalations.

6. Stages in a Cybersecurity Incident Response Plan

According to SANS Institute, the cybersecurity incident response plan contains six distinct stages. This plan helps IT professionals identify and deal with cybersecurity incidents such as cyberattacks. The stages include: (1) Preparation, (2) Identification, (3) Containment, (4) Eradication, (5) Recovery, and (6) Lessons Learned.

A fictional security incident scenario helps visualize and discuss these incident response stages. The scenario is an incident response plan for a phishing attack. Suppose that a fictional cybersecurity company—Securing the Inside—has developed an incident response plan in the event of a breach of their systems. Securing the Inside is internationally renowned for its services and the process by which they deliver these services to the end consumer. The company collects customers' personal information, including debit and credit card numbers and address information. Due to the sensitivity of this information, the company needs to protect the data. In terms of cyber threats, Securing the Inside is more concerned with e-mail-based phishing attacks. The following is an incident response plan to address phishing attacks the company might encounter.

6.1. Preparation

Preparation is the initial stage in this incident response plan. This stage involves laying a foundation and putting in place everything about responding to IT incidents. SANS institute lists multiple aspects of an incident response plan that should be prepared in advance. These include:

a. Policy – Having clearly written policies are essential; otherwise, the organization could face legal hardships. For example, an employee is on the company network, signs into their webmail account, and clicks on a suspicious email link. Afterward, a security incident is detected. Is checking webmail while on the company network allowed? Either way, a strict written policy avoids confusion and adverse effects.

b. Team - A CSIRT team will include personnel with expertise in IT, legal, and public relations fields. The IT team provides technical expertise in cybersecurity. The legal team offers legal counsel regarding any security incident. The PR team manages the dissemination of information about the breach to all Securing the Inside stakeholders and the public. The CSIRT team will be split into two groups, with each group represented by at least two individuals from every area of expertise. There will be two shifts—day and night, with each CSIRT group covering a shift.

c. Tools - Security information and event management (SIEM) systems monitor and alert personnel about phishing breaches. Also, the company deploys anti-phishing features in their email servers. These monitoring systems, built into the company's IT infrastructure, continually monitor for phishing activities.

6.2. Identification

Two elements act as sources of incident alerts: SIEM alerts and mailbox spam alerts. In case of a breach, the alerts go off, inviting the CSIRT team to the source of the breach. The CSIRT team examines the breach to determine its legitimacy. If the breach is legitimate, the CSIRT team initiates an analysis process to assess its severity and identify the details of the email. Analysis of severity involves examining the scope and impact of the attack on the company's resources. Analysis of the details of the email consists of gathering the email's header information (to know the sender's email, recipient's email, and the sender's IP) and message content (to check attachments and possible URLs).

6.3. Containment

Containment aims at mitigating the impact of the breach. Containment is either short-term or long-term. Short-term containment involves instant responses intended to stop the breach from spreading and causing more damage. One of the short-term practices is to isolate the

affected systems. Also, the CSIRT team blocks the sender's address in the company's systems. The address includes the IP address or the URL. Long term containment involves the restoration of essential systems back into operation without the affected systems.

6.4. Eradication

This process aims at removing all traces of the breach. Activities in this stage include deleting the phishing email from the company's systems and changing access logins of the affected systems.

6.5. Recovery

After successful eradication, the CSIRT team recommends when and how all the systems will be returned to operation. After restoration, the CSIRT team monitors all the systems, especially those that were affected, to ensure they are free from anomalies.

6.6. Lessons Learned

After the incident, the CSIRT team compiles all the activities about the phishing incident into a comprehensive report. The company's stakeholders review the report to understand the breach and its impact. In addition, the review will be used to come up with potential preventive measures. The following elements will be included in the report: when and who identified the breach; the scope of the breach; how the breach was contained; recovery activities carried out, areas where CSIRT was effective, and areas that need improvement.

7. Challenges in a Security Operation Center

As with every working team, a SOC faces challenges that are attributed to working together. By understanding the seven challenges of teamwork and their various perspectives, the team overcomes barriers and becomes a more cohesive group.

7.1. Building Trust

The first key challenge is *building trust*. Every great team needs to be comprised of individuals who trust each other. Without trust, teammates are not committed to supporting the group's efforts. Everyone has a bad day occasionally, so having reliable coworkers is essential. Without trust among team members, productivity drops. The SOC must run smoothly and

continuously. Even if productivity drops, alerts and events keep coming in. Someone must sift through these alerts. Will all teammates step up and pick up the slack? Or, will the responsibility be passed to the next shift? If a pattern ensues where the tasks are consistently left for someone else, team members start asking questions and wondering which individuals or teams are trustworthy. A lack of trust creates an environment in which no one wants to work. Communication slows down or comes to a halt, so information is not exchanged efficiently. The lack of communication results in duplicate work, missed alerts, and perhaps even a security incident. Ultimately, everyone does what benefits themselves, and all team members lack the motivation to work together.

Since trust is earned over time, overcoming the lack of it can be quite challenging. According to an article in Psychology Today, when comparing two sets of people, one group just talks small talk about the weather or what they ate for lunch. In this group, these individuals have known each other for many years. Then, the other group is comprised of individuals who have been working together for only a few months. This group is always talking to each other and working on fielding alerts. They bounce ideas off each other and share what they do for fun outside of work. The group that works closely with their peers has developed a bond, so they rely on one another. "Trust is built when our partners have the opportunity to let us down or hurt us – but do not. And in order for them to pass the test and build that trust, we must make ourselves vulnerable to that letdown" (Bonior, 2018).

7.2. Physical Proximity

The second key challenge in a SOC is *physical proximity*. With an increasing number of companies offering remote work, staying close physically proves to be difficult. Research recommends that teams work better when working in close physical proximity to one another. The study suggests that their local environment molds mammals. The COVID-19 pandemic forced the world to change its way of thinking and to do business. Businesses are coming up with new ways to interact. They are deciding the necessary frequency of meetings; and, once the meeting happens, what are the next steps for making decisions. If the process ends in disagreement and a need exists for further discussion, what does that process entail? This new outside the box thinking suggests there is a need for video calls instead of just audio calls. By having video calls, more in-depth conversations can take place.

7.3. Optimal Conditions

The next challenge is *optimal conditions.* Today, everything moves at a lightning-fast speed. Our organizations, teams, and technologies are ever-changing. Elaine Pulakos, an expert on organizational liveliness, states that there are three ways of handling this within an organization. Pulakos calls this "ARA" or "adaptability, resilience, and agility." A study was done by the Harvard Business Review, where they located a few companies that outpaced others. They discovered that the difference with these companies was instead of concentrating on serving their patrons and growing larger, they worked to mold humanity, had accidents, and strived to improve. To be able to do this, they concentrated on what is significant. Their process included reviewing which leaders are chosen, their leadership style, and past teamwork experience. There is always the need to move forward and change processes as they become outdated. Elaine Pulakos provides a few essential tips "look specifically at the individual behaviors that contribute to how the teams perform. And then consider whether the organization and attitudes toward working together are helping or hindering the ability to be agile, resilient, and adaptable." (Attfield, n.d.).

Applying "ARA" to a Security Operation Center can be reasonably straight forward. Is the SOC being asked to do more and more, but no new internal resources are available? If this is the case, the current processes and procedures should be reviewed. What systems are being monitored? What alerts are being generated and analyzed by the SOC? Are the daily and weekly reports that are currently being processed time-consuming? Of these, can some be eliminated to make room for a new task which may yield higher value? If not, why not? Does the team have strong performers who are eager to learn and do more? Are there less motivated individuals who may be a better fit elsewhere? Are there teammates who struggle with change or new processes? By taking a second look at these indicators, the focus can be redirected to the core duties, which may include intaking events, monitoring, hunting, and incident response. These ideas work toward improving the ARA.

7.4. Team Member Self-Awareness

Another principle challenge is *team member self-awareness.* When a larger group of people work together, more personalities surround the team. Some strong personality traits include individuals who are impervious to feedback, fault others for fiascos, and believe they

know everything. A study conducted by the Harvard Business Review determined that over 90% of people thought they were self-aware. The study showed different results. In fact, fewer than 15% of all employees are self-aware. People who fail to realize that they are not self-aware can hurt a team's success rate by nearly 50%. The study mentions that some aftermath triggered by the lack of self-awareness may include reduced initiative and increased stress (Hall, 2019).

First, to counter this, be sure that the colleague is, in fact, not self-aware. Is it possible that they are a bad worker? Could the wrong signals be due to a lack of communication or conflict of personalities? Is this person someone who can be trusted? Reasonable consideration must be given to determining the cause of the person's actions or the lack of effort. Perhaps this is something that can be remedied easily. Do this person's actions interfere with the ability of others to concentrate on their jobs? Would a simple request solve the problem? If any subtle efforts fail to address the issue, ask a few coworkers their impression of that individual. This inquisition would not be made to start gossip or rumors but to get the perception of others on the team. Quite likely, other workers have had similar issues with this person.

According to the author of the Forbes article, some common behaviors include:

- "Without realizing it, they say things that discourage people.
- They can't put themselves in someone else's shoes.
- They naturally become defensive with feedback or when someone brings up challenging questions.
- They have an overblown opinion of their performance and how they contribute.
- They aren't able to adapt how they communicate based on their audience" (Hall, 2019).

The most significant indicator that a person is self-*unaware* is that the person does not recognize their weaknesses. Generally, they try to be an effective team player. However, they do not realize that they are upsetting their peers. It is of the utmost importance to recognize that we can help people; however, if people do not want to change, we cannot do that for them. This choice will be up to them. By providing them this insight, the person can strive for greater self-awareness.

Applying these principles in a SOC would be the same as in any other industry. Everyone has different personalities. Some coworkers are easy-going; others are more difficult to get along

with and require more work. Remember that if issues arise, it is crucial to address them quickly and as they happen. A quick response helps the individual, the team, and the company.

7.5. Lack of Purpose

The fifth challenge is a *lack of purpose*. Kimber Lockhart (2016) states that "A sense of purpose is a deep understanding of the reason behind our efforts and a desire to pour in time and energy because that purpose resonates with the impact we'd like to make on the world." (Lockhart, 2016). When working in a security operation center, the question "Why are we doing this?" may arise.

For example, when a team repeatedly writes up the same alerts, the question will arise as to the reason these alerts are being triggered. Perhaps they are a signature match on something. Is the alert a false positive, and maybe the vendor needs to be notified? Or is this, in fact, an event that requires investigation. A SOC is not in the business to just write up alerts all day long. The SOC works toward determining 'why' these alerts are firing.

Telling the team "why" helps give purpose behind the big picture. Discussing the reason behind an action helps people understand what their hard work accomplishes and how it contributes to the goal. When team members know why they are doing a particular activity, they see that their work is meaningful and adds value to solve issues in the future. Most high performing teams of intelligent individuals find it challenging to put their ALL into something that they don't believe in or understand. The detail-oriented team wants to know and understand the purpose behind all their efforts, so they are more engaged in their work.

7.6. "Negative Nancys" or "Negative Neds"

The sixth challenge is "*Negative Nancys" or "Negative Neds."* Every work environment seems to have one on their team. They spread a gloomy boldness that binges among the team. If there is a difficult task coming ahead, these individuals are very vocal. They will criticize everything; more than likely, they will not offer any solutions. These team members bring down morale and cause conflict. Positive suggestions made by the manager or other coworkers tend to combat their negativity. If an upcoming new task has been tried with less than great success, present the idea again by saying, "we have made some changes, and it is going to work this time because of these changes – Let's give it a shot again" (Hansen, 2016).

"Negative Nancys" or "Negative Neds" in the SOC bring down the team of cyber professionals. Some complaints include:

- Why are we writing up these alerts?
- Why do these tools never work?
- Perhaps one of the shifts or a team member is not contributing.
- We never get any training.
- The training we get is never on my shift.

The list of complaints goes on and on. "Negative Nancys" or "Negative Neds" are team members who need some special one-on-one assistance. The manager can gain their support by pulling the team member aside and letting them know the importance of their role and contributions to the current jobs. A good manager needs to inform them that their behavior affects the entire team, but that their concerns are valid and warrant attention. Often, negative team members may offer potential solutions and start to be positive as the team is slowly reshaped.

7.7. Taking the Pain Out of Meetings

The final challenge is *taking the pain out of meetings*. A meeting can be a great thing; however, meetings should not magically pop up on the company calendar. For example, an employee should not leave the office on a Wednesday evening with no meetings only to arrive on Thursday and find that two new meetings have cropped up. Certainly, those required to attend wonder, "What is this meeting?" and "Why is it scheduled during lunch hour?" All employees are busy completing day-to-day tasks and now must also manage meeting nightmares.

A few things take the pain out of these meetings. First, all meetings need to have an agenda. With the agenda, the person leading the meeting can make sure to invite all people who need to attend and have all the necessary resources on hand. Only invite those parties who are going to assist with moving the project on the agenda forward. No other groups of people need to attend. Perhaps, before scheduling the meeting, various groups should be contacted individually. A decision-maker can help significantly during a meeting. First, all the resources must be collected, and attendees identified. Then, the leader must decide what needs to be accomplished at the meeting.

Josh Higgason, jhiggason@gmail.com

The next essential item is to use everyone's time wisely. After the agenda has been sent, attendees can come to the meeting prepared. By requesting their preparation before the meeting, more can be accomplished. Everyone knows what is expected of them. They can provide their input without a need to try to come up with things ad hoc.

Sometimes meetings get hijacked or off track. For the meetings to be beneficial and things to be accomplished, the attendees must remain focused on the topic. If a meeting is going to last for an extended period, attendees will need breaks. By taking a break, the leader has time to recap and state what will be covered next. This recap and following break refreshes everyone's memory and brings them up to date.

During and immediately following the meeting, the leader may solicit feedback. The attendees provide input about what went well and what they would like to see done differently next time. Their responses help with planning future meetings. Finally, the leader must note what action items are needed and assign tasks to internal and external attendees. Once task assignments have been made, attendees must be held accountable for things moving forward (6 Common Team, n.d.).

8. Conclusion

The history of cybercrime goes back almost 200 hundred years with roots set by two wise bankers and a telegraph operator. Then in the mid-1950s, the trend continued with individuals tricking the phone system into making free long-distance phone calls. In the 1980s, the CIA implanted a logic bomb that affected the Siberian Gas pipeline. The list goes on and on getting more complicated as technology advanced.

Threats such as phishing, DDoS, and data compromise have impacted businesses and the economy. Further, Qakbot, and COVID-19 directed campaigns and cyber-security breaches threatened data integrity.

A Security Operation Center requires many different team members, each with a precise role. The teams are divided using the tier system. Those employees on a tier-one team assist with triage events and alerts. A tier two team reviews IOCs and tracks down affected assets. Tier three team members find threats inside the company and recommend ways to improve current security tools. Finally, there is a SOC manager that leads the team and works to discover new talent and provide appropriate training.

The Security Operations Center faces seven key challenges that must be overcome. These challenges include building trust, physical proximity, optimal conditions, team member self-awareness, lack of purpose, negativity, and holding purposeful meetings.

References

6 common team challenges – How to overcome them and grow your team – Bytestart. (n.d.). Bytestart. https://www.bytestart.co.uk/tackle-common-team-challenges-develop-team-performance.html

Attfield, B. (n.d.). 5 challenges of teamwork (and how to overcome them). Employee Engagement and Internal Communication Blog | Jostle. https://blog.jostle.me/blog/5-challenges-of-teamwork-and-how-to-overcome-them

Bonior, A. (2018, December 12). 7 ways to build trust in a relationship. (2018, December 12). Psychology Today. https://www.psychologytoday.com/us/blog/friendship-20/201812/7-ways-build-trust-in-relationship

Cimpanu, C. (2019, July 4). *Hacker who launched DDoS attacks on Sony, EA, and steam gets 27 months in prison*. ZDNet. https://www.zdnet.com/article/hacker-who-launched-ddos-attacks-on-sony-ea-and-steam-gets-27-months-in-prison/

Cynet (n.d). Incident Response SANS: The 6 Steps in Depth. https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

Developing story: COVID-19 used in malicious campaigns. (2020, April 24). Trend Micro | Enterprise Cybersecurity Solutions. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Hall, J. (2019, February 20). *How to work with people who aren't self-aware.* Forbes. https://www.forbes.com/sites/johnhall/2019/02/17/how-to-work-with-people-who-arent-self-aware/#

Hansen, B. (2016, May 24) *6 challenges to team collaboration*. Powerful, Versatile Work Management Platform | Wrike. https://www.wrike.com/blog/6-challenges-team-collaboration/

Lockhart, K. (2016, February 10). *Don't create a sense of urgency, foster a sense of purpose*. Medium. https://medium.com/@kimber_lockhart/don-t-create-a-sense-of-urgency-foster-a-sense-of-purpose-724e309ecdb0

Oliver, M. (2018, May 14) *10 early hackers from before the invention of the home computer*. (2019, June 9). Listverse. https://listverse.com/2018/05/14/10-early-hackers-from-before-the-invention-of-the-home-computer/

Pajares, C. (2020, May 4). *Phishing, other threats target email and video app users.* Trend Micro | Enterprise Cybersecurity Solutions. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/phishing-other-threats-target-email-and-video-app-users

Standage. T. (2017, October 5) *The crooked timber of humanity*. 1843. https://www.1843magazine.com/technology/rewind/the-crooked-timber-of-humanity

Swinhoe, D. (2020, April 17). *The 15 biggest data breaches of the 21st century*. CSO Online. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

The 10 costliest cyberattacks in the history. (2015). Lifars https://lifars.com/2015/06/the-10-costliest-cyber-attacks-in-the-history-of-internet/