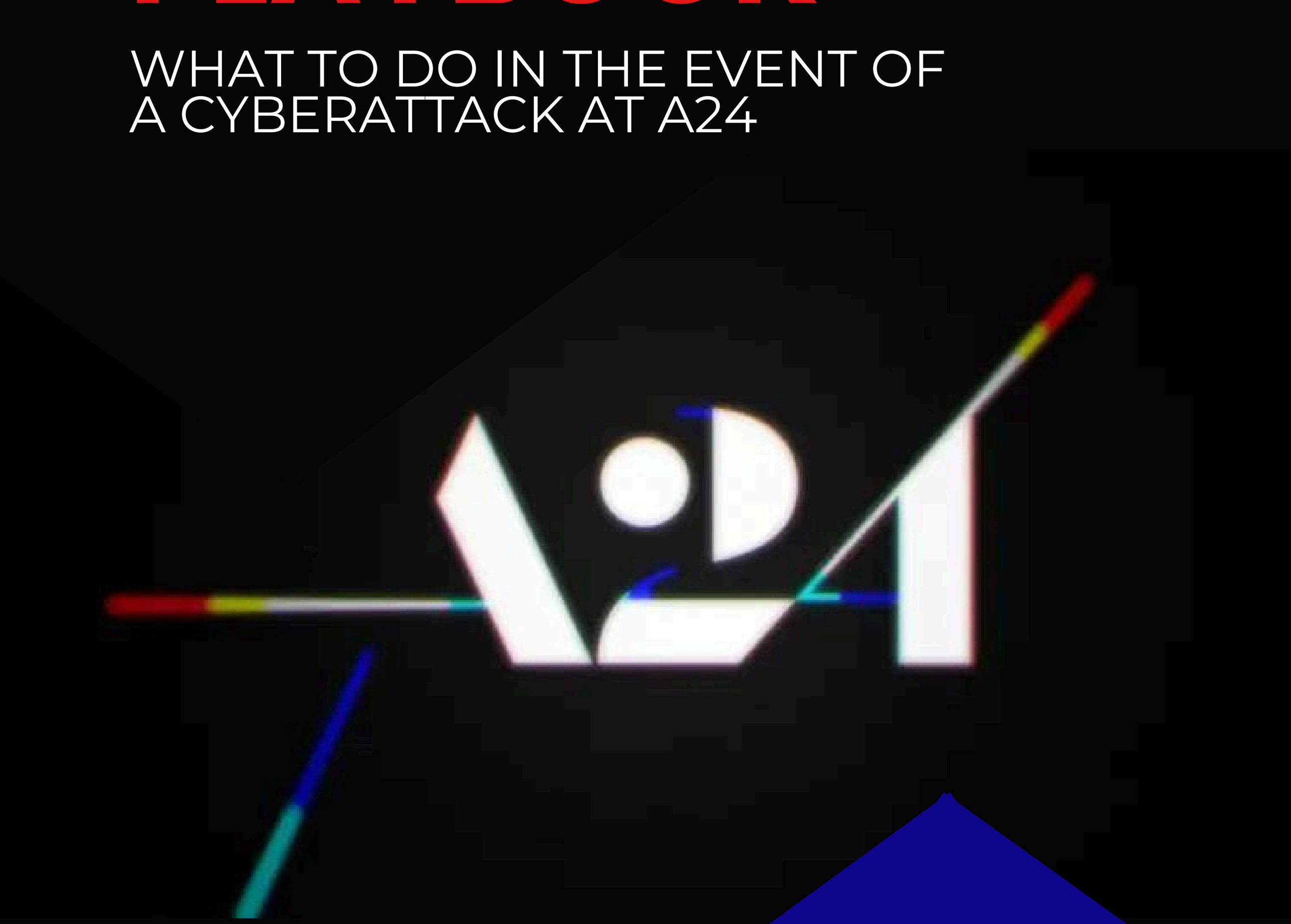
MariCarmen Mosso Co.

THE CYBERSECURITY PLAYBOOK

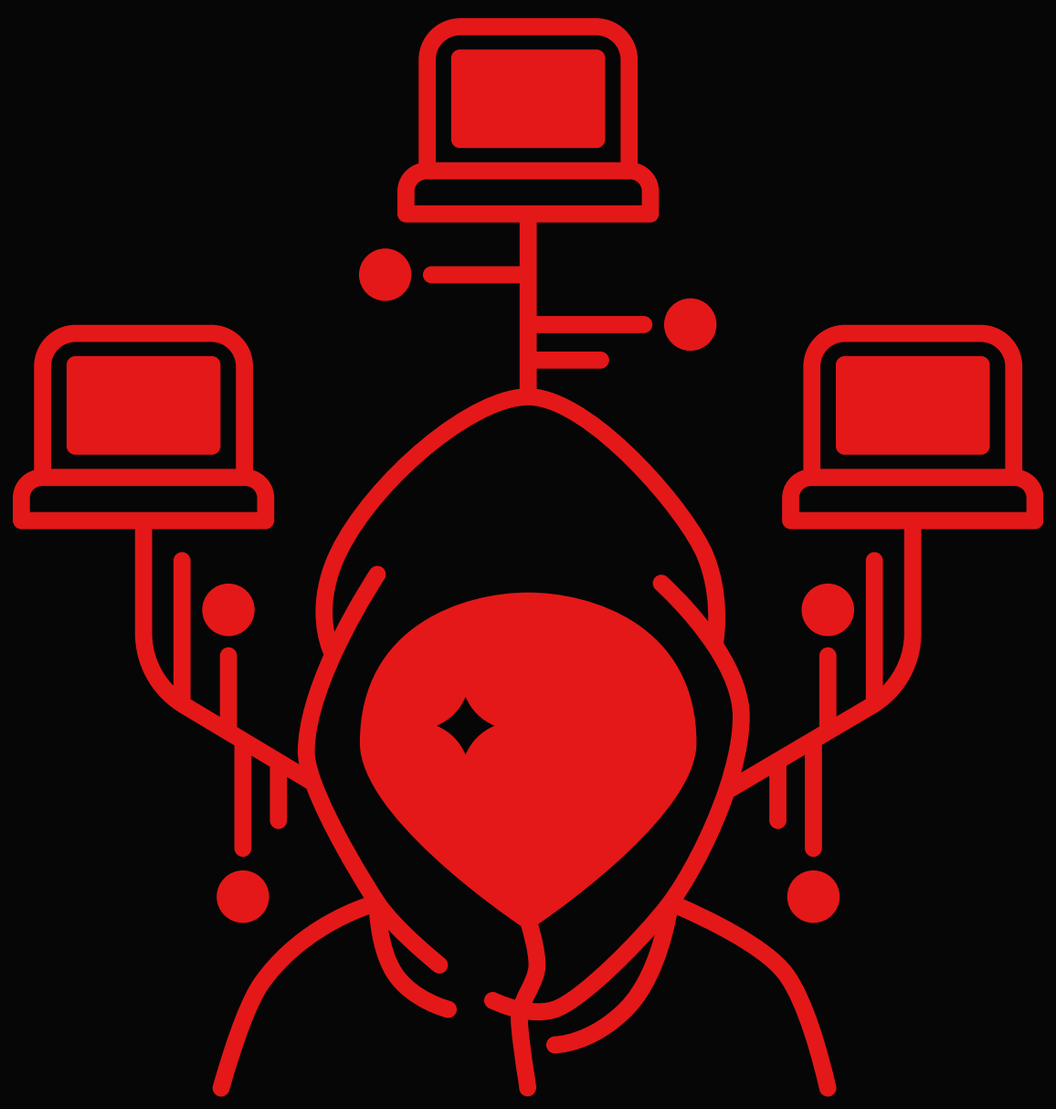
WHAT TO DO IN THE EVENT OF A CYBERATTACK AT A24



2024

LETS KEEP FILM SAFE!

PART 1:
SECTION 1: DESCRIBING A POTENTIAL CRISIS



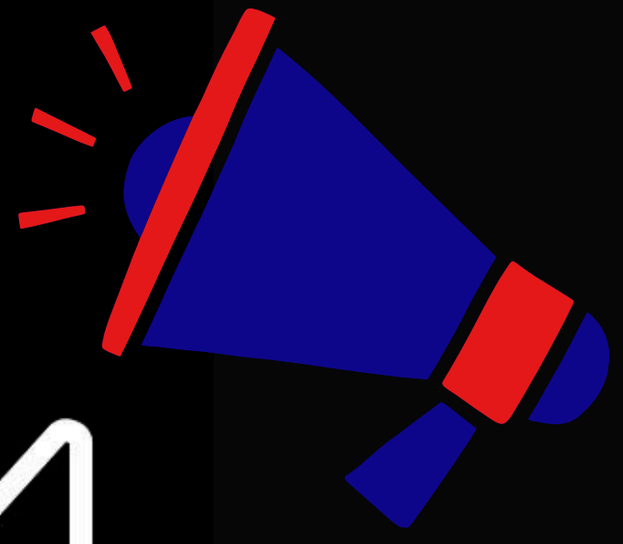
The Scenario:

Over the weekend, A24 has fallen victim to a sophisticated ransomware attack. The hacking group WebWeavers were able to infiltrate A24's internal network, encrypting critical data, including unreleased film footage, confidential contracts, and sensitive personal information of A-list cast and crew, as well as fans that pay $5 a month to be subscribed to A24's fan program. The group was able to infiltrate the company through a cybersecurity attack known as "Whaling." By targeting the company's CFO, the group disguised themselves as an independent filmmaker hoping to gain more experience through connecting with top executives in A24, hoping to learn about the company before deciding to work with them. They educated themselves with information about the CFO's past, and connected with them by saying they had gone to the same university and both were from the same town. The LinkedIn profile of the fake persona the hackers engineered to trick the CFO into trusting them was highly sophisticated, with 500+ connections, film experience, and a name that was connected to other forms of social media. As a result the CFO believed the farce, and gave minimal internal access to the persona, but this minimal access was enough for the hackers to put one foot though the door. Now, the hackers are demanding a substantial ransom, payable in bitcoin, and if the ransom is not paid, they will permanently delete all encrypted data and release sensitive information to the public. The cyber attack has gained national attention, which has led to a significant drop in the company's stock price and growing public concern about the safety of their personal data.

In an attempt to respond to the crisis, the company's executive team must act quickly and decisively to manage the crisis before it becomes unbearably big. At the moment, the CEO is under immense pressure from shareholders, the public, and the media to address the situation effectively in order to maintain the company's reputation. Fans feel as though they have been let down by their favorite company, and now even lack trust in the company. Now, how the CEO manages the crisis under the scrutiny of the public eye will be crucial to the company’s reputation. While the CEO works with executive communication officials within the company, the CISO is tasked with leading the technical response to the attack, and the COO must focus on maintaining operational continuity. This, is in depth, the steps that should be taken to ensure full transparency, and a full A24 recovery, from this attack.

We are all fighters in this battle to save our company and protect films and film fans everywhere!

SECTION 2: CEO'S STEPS AND DECISIONS

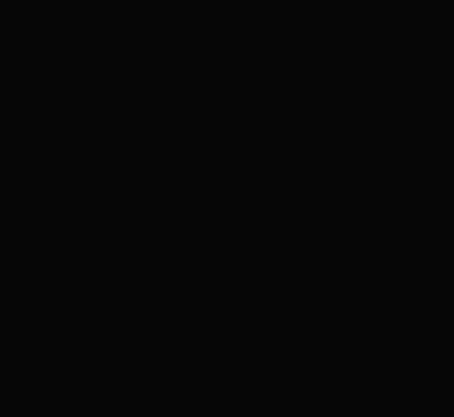


The CEO must take immediate action to manage both the internal and external aspects of the crisis. Initially, the CEO must convene an emergency meeting with the board, executive team, including the CISO, COO, CFO, and legal counsel, in order to gather all available information about the attack and establish a unified response strategy by following the predefined procedures they had learned about through the company's annual cybersecurity informational sessions. The CEO needs to communicate transparently with stakeholders, employees, shareholders, and the public, to maintain trust in the company. This involves issuing a public statement acknowledging the breach, outlining the steps being taken to address it, assuring stakeholders of the company's commitment to resolving the issue, and maintaining its commitment to fans to continue to give them the highest quality service and content.

Additionally, the CEO should contact law enforcement and the cybersecurity team within the company, in order to ensure that the company continues to comply with legal requirements, and works with law enforcement in order to track down the hacking group, bringing them to justice so that this type of crisis does not happen again, nor does it happen to another company. Since the CEO is considering paying the ransom, mainly to regain control of the affected subscribed fan's and A-list celebrities' information, the CEO must first obtain approval from the board. This is to consider the potential risks and benefits of such a decision, as there are ethical implications and potential future vulnerabilities that paying a ransom might create. The CEO must consistently update the board and stakeholders as well, ensuring that response efforts are well-coordinated and the company can make a full A24 style comeback.

SECTION 3:

CISO'S STEPS AND DECISIONS



A24

The Chief Information Security Officer, the CISO, is now at the forefront of the technical response. They are responsible for leading the investigation and mitigation efforts with law enforcement. When the attack first occurred, the CISO worked with the IT department and cybersecurity teams to isolate affected systems to prevent the malware from spreading further. Luckily, they were able to shut down compromised networks rather quickly, including the shop A24 website, and deployed advanced threat detection tools to identify the attack's origin, which they were able to track down to the fake persona the CFO was talking with. During this process, the CISO must manage the cybersecurity team’s effectiveness during the crisis, ensuring that all efforts are well-coordinated, and the situation is being managed as quickly as possible. This would include assigning clear roles and responsibilities to the team, providing the necessary resources, and facilitating collaboration with other departments such as finance and technology.

While all of this is taking place, the CISO must also be in close contact with the CEO, other executives, and board members, keeping them up to date on the state and severity of the situation. Once the immediate threat of the attack has been contained, the CISO should now work with the CEO and focus on implementing more enhanced cyber security measures. These measures could include improved network segmentation in order to limit the spread of malware if attacked again, regular employee training on identifying and responding to phishing and whaling attacks, and the continuous monitoring of the company’s digital environment.

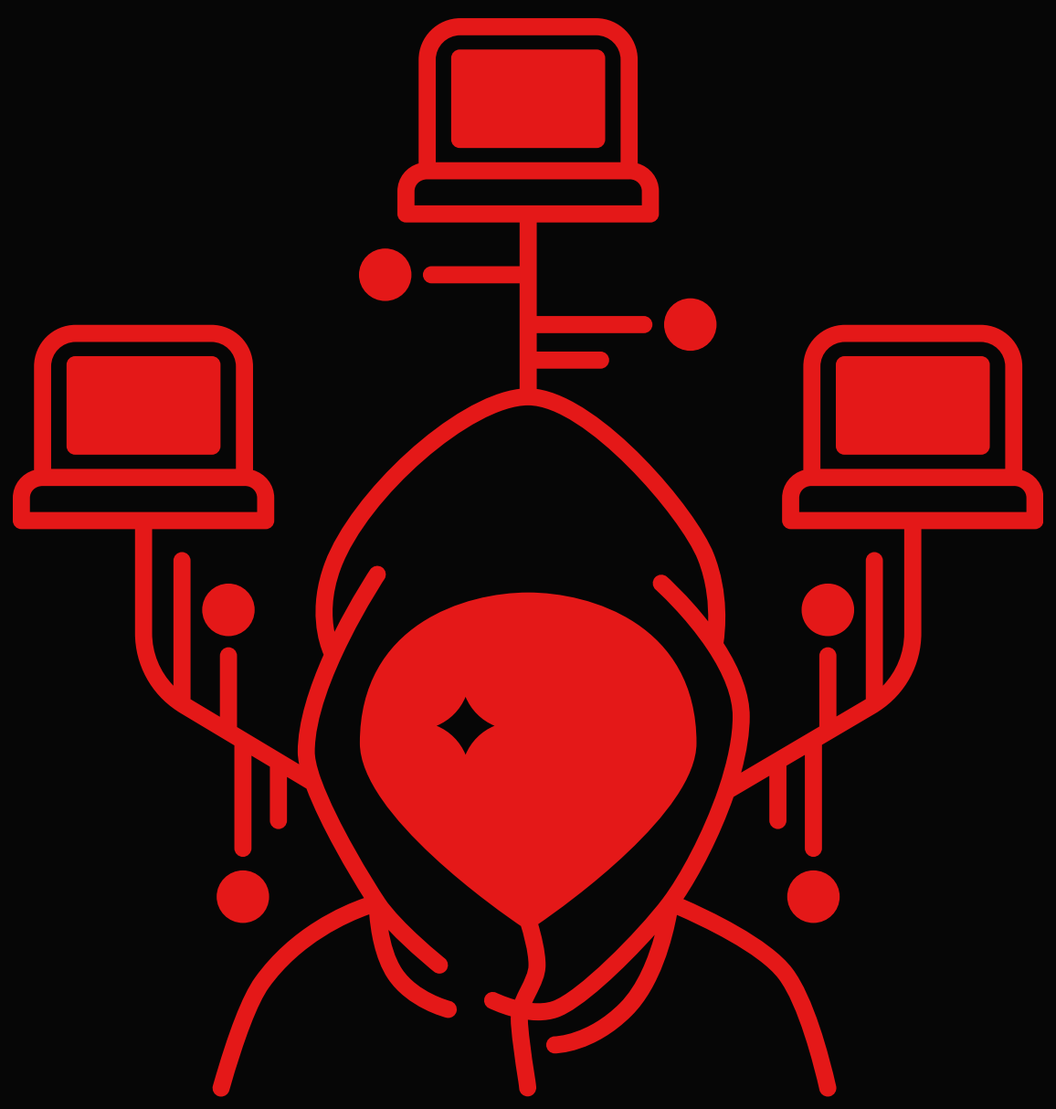
SECTION 4: COO'S STEPS AND DECISIONS

A24

In the film industry, every second matters, and a disruption to production and filming schedules could cost the company and all the people involved thousands of dollars for every second lost. It is the job of the COO, Chief Operating Officer, that operations can continue where necessary, without making any other area of the company vulnerable to a secondary attack. In the immediate aftermath of the attack, the COO must work closely with the CISO in order to understand the full extent of the breach and assess its impact on the company's operations. This includes identifying which production systems and administrative functions have been affected and determining if any alternative methods can be implemented to maintain business operations as usual. The COO should follow the company's contingency plans, which may involve shifting critical tasks to unaffected systems, implementing manual processes where possible, and reallocating resources to support essential operations.

Another key task for the COO is to oversee the establishment and maintenance of reporting systems that keep all stakeholders informed about the operational status and recovery progress of the company, as the news of the cyberattack has hit A24’s stock prices very hard. The COO must set up regular briefings with other executives in order to gather updates and ensure that accurate information is communicated to the CEO, the board, and the company’s stakeholders. The COO must also ensure that any changes to operational procedures are well-documented and that staff are informed and trained on any new protocols, and cybersecurity measures, to prevent any other further disruptions.

PART 2: SECTION 1: REGULATOR AND LAW ENFORCEMENT NOTIFICATION



Managing the cyberattack is only the first part of our uphill battle, as there are numerous legal regulations that have to be considered when responding to the crisis. Following the cyberattack, the immediate steps will involve notifying the relevant regulators and law enforcement agencies, letting them know in as much detail as possible what has taken place at our precious company. The Chief Legal Officer must ensure compliance with legal requirements under data protection regulations, such as the GDPR, which mandates that the breach must be reported to the Information Commissioner's Office within 72 hours. The report submitted should include the nature of the breach, the types of data affected (including personal data of cast and crew, fan subscribers, and leaked information about the movie), the number of individuals impacted, and the immediate actions we have taken to contain and mitigate the breach, keeping A24 as safe and protected as possible.

Simultaneously, our Chief Legal Officer should be preparing to submit a report to the Securities and Exchange Commission in the form of an 8-K filing, detailing the breach, its impact on the company's financials, and the steps we have taken to address the situation at hand. So in this case, a report detailing how the CFO was victim to "Whaling," and the repercussions that followed, including the hefty ransom amount the WebWeavers are demanding. Following this report, law enforcement, such as the FBI, should also be contacted to investigate the ransomware attack, track the WebWeavers, and support recovery efforts. Remember we must bring down the *Iron Claw* on our cyber attackers.

A statement should also be crafted for public disclosure, which acknowledges the breach, outlines our extensive and full commitment to resolving this issue, assuring both stakeholders and our loyal fans that law enforcement and regulators are involved. This statement will help manage our public relations while maintaining transparency and trust. We must not let this breach overshadow whatever upcoming film we have slated, but we must ensure everyone that it is our number one priority. Additionally, it is crucial to keep detailed minutes of decisions made during the crisis and ensure that legally privileged discussions with outside law firms can take place to protect sensitive information. In terms of our commitment to solving our cyberattack,we must make sure we deal with *everything everywhere, all at once*.

SECTION 2: LEGAL CONSIDERATIONS IN PAYING A RANSOM

A24

In the scenario described, WebWeavers are demanding a hefty amount in ransom payable only in bitcoin. If the stolen data cannot be recovered, and paying the amount is being considered as the only option, it is crucial to follow a defined legal process. It unfortunately is not as simple as paying the ransom and having everything drift away into the *moonlight*. The decision to pay the ransom must be an executive decision made in advance with all jurisdictional restrictions and ethical implications considered along with the well being of the company's future. If the decision is made to pay the ransom, the CLO must ensure that proper legal steps are taken, such as verifying the legality of the payment, coordinating with finance to secure the bitcoin payment, and keeping detailed records of all decisions to verify all proper legal steps were taken with the FBI.

Another thing to remember and consider is vicarious liability, meaning A24 may be held liable for third-party damages resulting from the breach, depending what data was affected. While in the scenario given there is no mention of the data affecting a third-party company, if a different cyber attack were to happen where that was the case, it would be of the utmost importance to take note of that. For example, if a different cyberattack on A24 spread to a client like AMC theaters, which shows our movies, the company must evaluate its liability and determine if liability caps in contracts offer protection. Similarly, if a supplier's breach, such as a background screening provider, leads to the loss of employee data, A24 must assess its responsibility and legal obligations. However, since in the scenario given some of our customer's data was affected, these customers could take legal actions against our company depending on the data that was compromised and lost.

Lastly, the CLO must also ensure that all relevant regulators and law enforcement agencies are informed. For large multinationals, identifying a lead regulator or law enforcement agency is essential. Ensuring SEC reporting requirements are followed is a key responsibility. During the crisis, the legal team must balance restoring operational systems with preserving evidence to prove any loss or damage to employee or customer data.

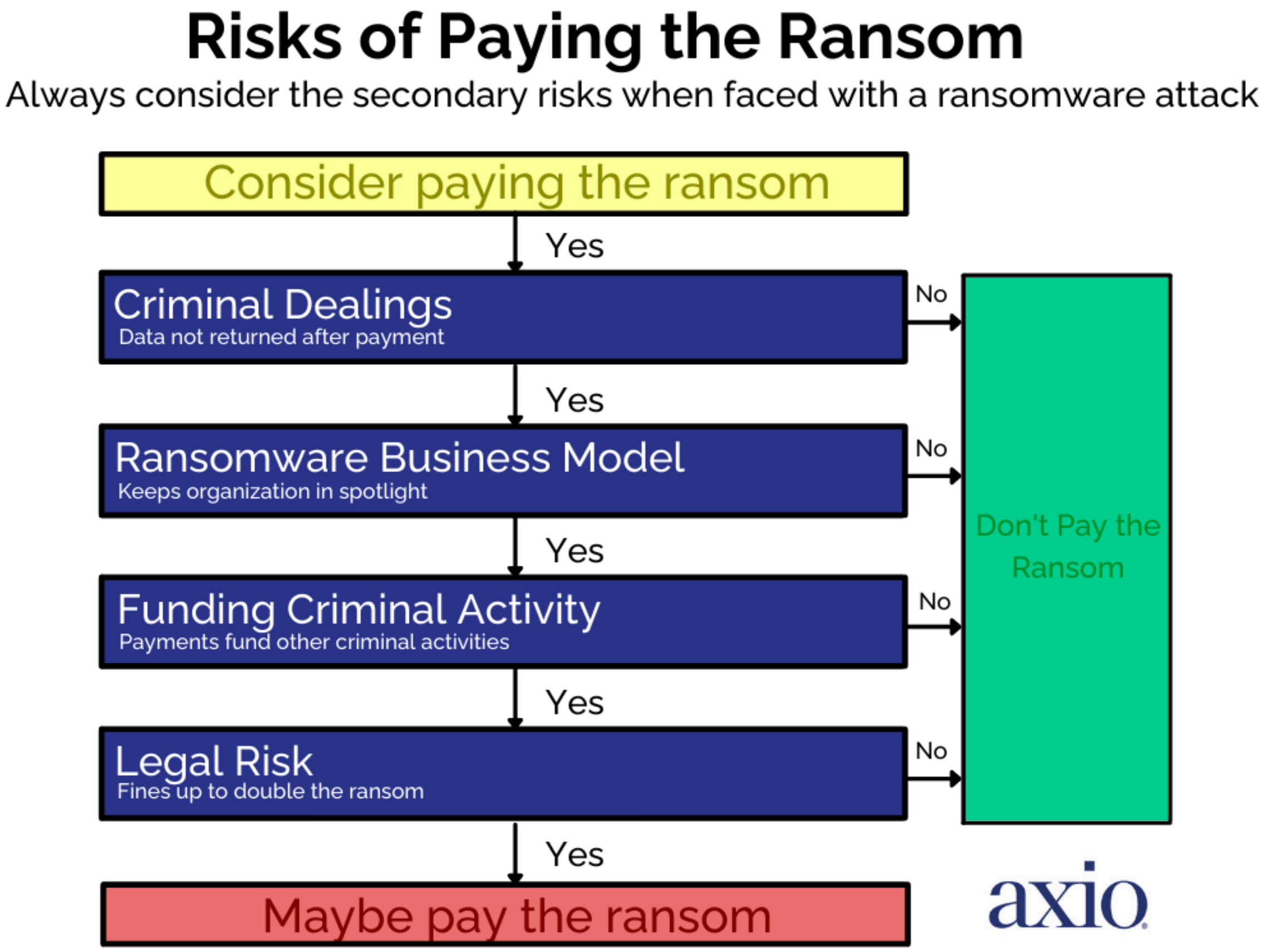


*image from axio.co

SECTION 3: FINANCIAL IMPLICATIONS OF DECISIONS DURING A CYBER CRISIS

A24

In the aftermath of the ransomware attack on A24, financial trade-offs need to be carefully considered. If our company halts production for one day, the immediate financial loss will include lost revenue and increased costs for temporary filming solutions. Movies are made on a tight schedule, and any loss of time would be consequential. Even a two-day production stoppage could significantly impact revenue, operational efficiency, and client relationships. However, restoring systems and filming too quickly without a thorough investigation could also have financial implications, such as additional data loss or further exposure, leading to prolonged operational disruption and increased recovery costs. There is a thin line to walk in deciding what is best for our company, our filmmakers, actors, operational workers, and film lovers. Every piece of our A24 puzzle is important and must be considered.

In all, this is why cybersecurity info-sessions, and the creation of this playbook is extremely important to prevent any cyber crisis before it takes place, and if it does take place, being able to respond in the most effective manner. *We live in a time* where investment in robust cybersecurity measures and comprehensive insurance coverage is necessary to help mitigate these financial risks, providing a buffer against the economic impact of the breach and facilitating a faster, more effective recovery. Being as knowledgeable on the topic, and being as prepared as possible, is the only way to protect ourselves in this ever-changing technological world, and continue to bring our movies to our fans.