MAKE THE
WORLD SEE

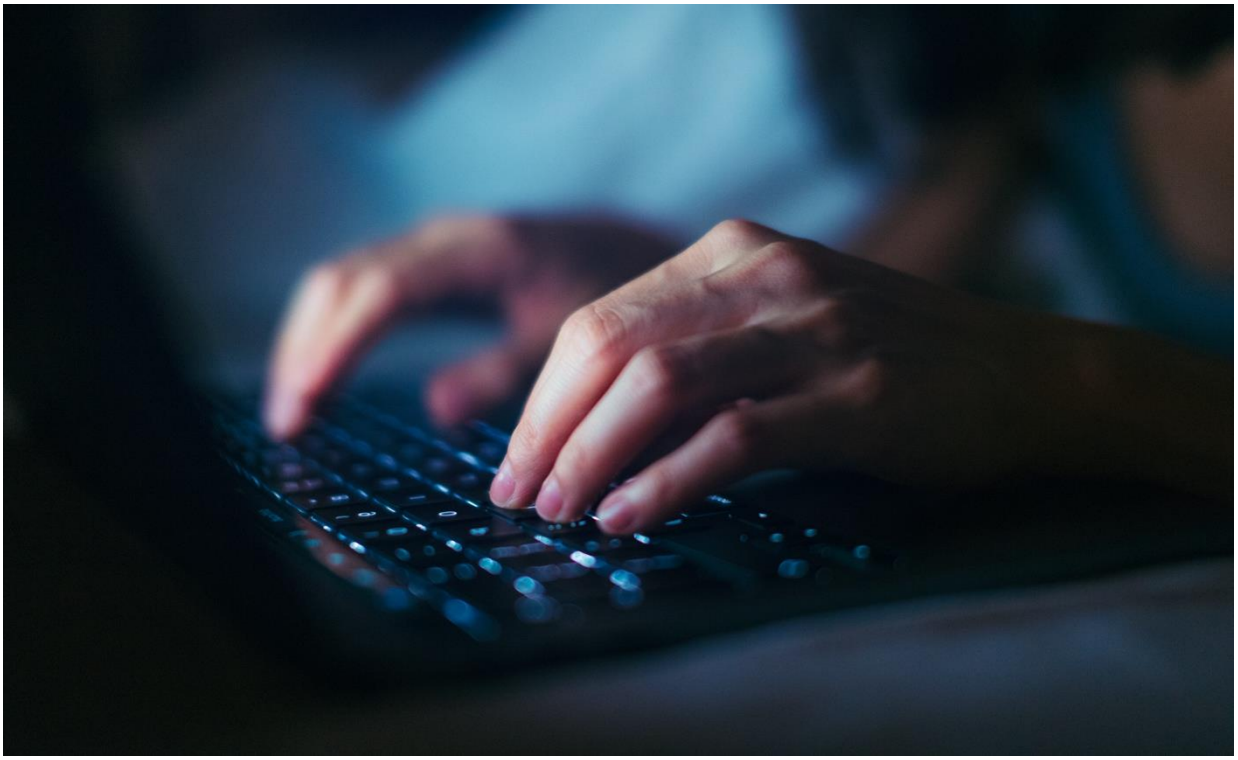
Thought Paper

Cybersecurity for video technology

Understanding and countering cyber threats

milestone

Table of contents



On Guard: Navigating Cyber Threats in Video Technology

In an era where even your video technology solutions aren't safe from cyber threats, neglecting cybersecurity is akin to leaving your front door wide open. The 2021 breach into Verkada's surveillance system is a chilling testament to this reality. The hackers didn't employ sophisticated artificial intelligence (AI) or powerful algorithms; they simply found a username and password exposed in the public domain. This incident should jolt us into a new awareness of the crucial role for cybersecurity in video technology.

This Thought Paper addresses the urgent need for robust cybersecurity measures in video technology solutions. Aimed at technology decision-makers considering video surveillance solutions, we will navigate together through the world of potential threats, preventive measures, and effective strategies to fortify your video technology solutions.

Executive summary

In this digital age, cyber threats are an escalating concern, particularly for video technology solutions. A recent breach into Verkada, a prominent surveillance company, and the subsequent unauthorized access to a variety of sensitive data has highlighted the critical need for robust cybersecurity measures.

This Thought Paper provides a comprehensive guide on understanding and countering cyber threats, specifically tailored for technology decision-makers in the security industry. By delving into the concept of the Cyber Kill Chain, it explains the stages of a cyberattack and corresponding preventive measures to counter each stage. Additionally, it discusses the specific vulnerabilities of IP-network video cameras and Video Management Software (VMS), and the importance of proactive and layered defenses.

Lastly, the paper emphasizes the crucial role of the human factor and the significance of education, training, and a balance between security and usability. This paper offers valuable insights to help you navigate this complex landscape of potential threats and effective strategies to strengthen video technology solutions against cybersecurity attacks.

Surprisingly simple to breach the system

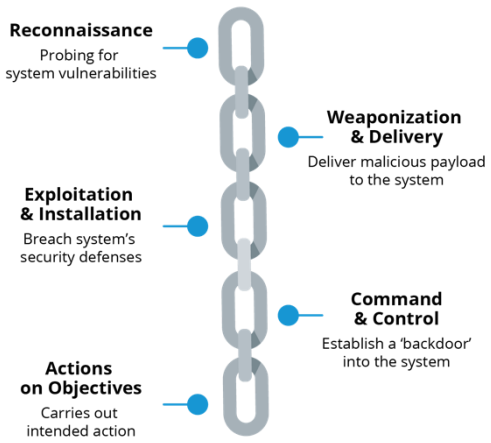
In March 2021, a security breach involving Verkada, a prominent video surveillance company, underscores the scale and potential impact of such incidents. With a diverse portfolio of high-profile clients, including Tesla and Halifax Health, Verkada fell victim to hackers who gained access not only to video recordings but to a comprehensive list of thousands of clients and critical financial information.

The breach into Verkada's surveillance systems was surprisingly straightforward, highlighting alarming vulnerabilities in the company's security infrastructure. The group of hackers were able to gain super admin-level access to Verkada's systems by discovering a username and password for an administrator account publicly exposed on the internet. This level of access allowed them to peer into the live video feeds of all Verkada's cameras and gain entry to a treasure trove of sensitive data. The incident serves as a stark reminder of the importance of robust cybersecurity measures, even for seemingly secure systems.

As you navigate this complex landscape, safeguarding your company's people, assets and reputation is of paramount importance. This begins with understanding the stages through which a cyberattack progresses, the inherent risks at each stage and the right cybersecurity measures to counter the attack. So, how does your organization go about comprehending these risks and implementing the appropriate measures? Enter the Cyber Kill Chain.

The Cyber Kill Chain in Video Technology

The Cyber Kill Chain, a concept first introduced by Lockheed Martin, provides a systematic framework for understanding and countering cyber threats. It breaks down a cyberattack into seven progressive stages: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives.



Understanding these stages helps to reveal the attacker's strategy, predict their next move, and ultimately prevent or mitigate the attack. Implementing defenses at each stage can significantly reduce the likelihood of a successful cyberattack on your video technology solution. For instance, during the 'Reconnaissance' stage, a hacker might identify IP-network video cameras as a potential target and gather information about their location and vulnerabilities. In response, companies could implement measures to detect and prevent such reconnaissance activities, such as intrusion detection systems or regular system audits.

Cybersecurity Strategies Across the Cyber Kill Chain

When it comes to cybersecurity for video technology, it's crucial to understand that protection isn't a one-step solution; rather, it is a multi-tiered strategy addressing all stages of the Cyber Kill Chain.

Reconnaissance: The first stage involves the cybercriminal probing for system vulnerabilities. To counter this, companies should ensure their systems are invisible to port scans, which can be achieved with security measures like firewalls and intrusion detection systems.

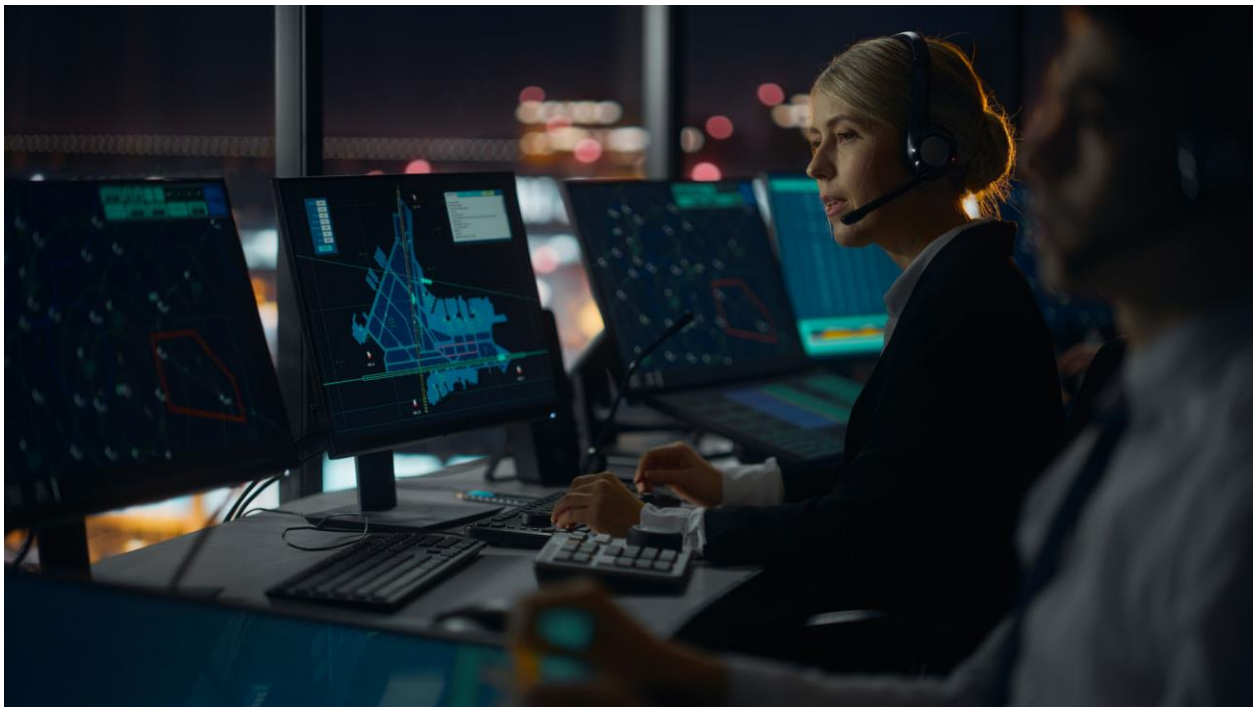
Weaponization & Delivery: Hackers create a malicious payload and deliver it to the target system. Defenses at this stage include robust email security to prevent phishing attacks, frequently updating and patching systems to fix known vulnerabilities, and implementing strong controls over Universal Serial Bus (USB) and other physical interfaces.

Exploitation & Installation: The stage where the attacker breaches the security defenses. Companies can defend against these activities by installing advanced endpoint protection solutions, which employ machine learning to identify and block novel threats.

Command & Control: This is when hackers establish a 'backdoor' into the compromised system. To detect such activities, network activity should be continuously monitored for any unusual patterns or communications with known malicious IP addresses.

Actions on Objectives: The final stage where the attacker carries out their intended action. Regular system audits and data backups can limit the damage and speed up recovery in case of a successful attack.

By understanding the Cyber Kill Chain and implementing defenses at each stage, companies can significantly enhance the security of their video technology solutions. Proactive and layered defenses can deter attackers, detect ongoing attacks, and minimize the impact of successful breaches.



Protecting an airport – a scenario

To illustrate the relevance of a proactive cybersecurity approach based on the Cyber Kill Chain, consider the following fictitious scenario that shows how an airport might utilize a multi-faceted approach to secure their video technology solution. Recognizing the potential vulnerability of an extensive network of security cameras to cyberattacks, the airport should implement a layered defense strategy aligned with the stages of the Cyber Kill Chain.

During the reconnaissance phase, leveraging advanced threat intelligence and intrusion detection systems to predict and deter threats. For the weaponization and delivery stages, having IT teams employ cutting-edge firewall technologies to prevent malware from penetrating systems.

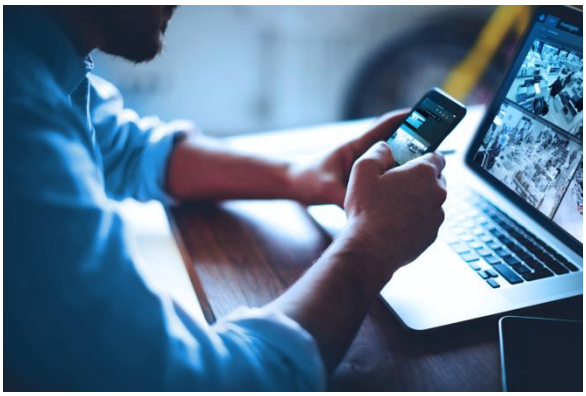
In the event of a successful breach, the security measures still offer protection. During the exploitation and installation phases, using endpoint protection strategies, powered by machine learning, to identify and neutralize harmful software. For the command & control and actions on objectives stages, the airport should monitor network traffic to detect any unusual patterns, indicating potential control and command activity.

Finally, regular audits of information systems must be conducted to ensure the robustness of the cybersecurity measures. This scenario demonstrates how a comprehensive, layered cybersecurity strategy can protect valuable video technology solutions from potential threats.

Note: this scenario is intended to illustrate how to use multi-layered approach to counter cyber criminals, it is not based on a real study.

Protecting IP-Network Video Cameras

IP-network video cameras play a crucial role in ensuring security. However, they can also pose potential risks by serving as gateways for unauthorized access to your company's network. One significant vulnerability is the transmission of unencrypted data, which can be intercepted and viewed by malicious parties. This vulnerability must be addressed to mitigate the associated risks. Additionally, insecure mobile applications can serve as easy entry points for hackers due to their lack of robust security measures.



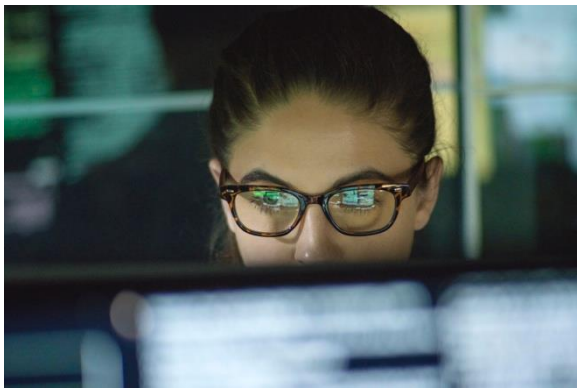
To prevent unauthorized access, it is essential to implement strong authentication protocols. Relying on default passwords is a glaring vulnerability that should be avoided. The Cybersecurity Infrastructure Security Agency (CISA) suggests changing default passwords as a simple yet effective step towards enhancing security. Regularly updating firmware is also crucial to address any potential security flaws.

By proactively addressing these common vulnerabilities in IP-network video cameras, you can increase protection for your organization from cyber threats. This not only safeguards your video technology solutions but also strengthens your overall network security.

Protecting Video Management Software

Video Management Software (VMS) is the core of modern video technology solutions and protecting it from cyber criminals is of paramount importance. This involves a multi-faceted approach, encompassing penetration testing, the use of ethical hackers, and implementing containment strategies.

Penetration testing



In addition to development teams creating and securing new software, vendors must also have teams dedicated to breaking into, or penetrating their systems. This is a crucial step for every new release and update. Ethical hackers, often referred to as "good guys," are external teams who attempt to break into systems to identify vulnerabilities and improve overall security.

Do vendors employ ethical hackers to assess their systems? Ethical hackers sometimes test systems without the manufacturers' knowledge and

subsequently inform them of any vulnerabilities they discover. While some companies promptly address and fix these issues, others may not take immediate action.

Defense in depth

To mitigate the consequences of an attack, software solutions must be secured at multiple layers, to create redundant security controls. By doing so, if a hacker manages to breach one part of the solution, the impact remains limited to that specific segment, preventing unauthorized access to other areas.

This defense in depth strategy serves two purposes. Firstly, it facilitates the auditing process, enabling a thorough investigation to identify the actions taken by the attacker and when they occurred. Secondly, it allows for a post-mortem analysis, helping administrators to analyze the intricacies of the attack, comprehend the underlying causes, and devise preventive measures against similar future attacks.

Who's responsible for cybersecurity?

Understanding the clear distinction between who is responsible for what in terms of cybersecurity for on-premises and cloud solutions is essential. While on-premises solutions place the responsibility of cybersecurity squarely on the customer's shoulders, cloud solutions transfer that responsibility to the vendor. Each approach has its unique advantages and challenges for cybersecurity, specifically considering the critical importance of video data.

On-premises

In the domain of on-premises video technology solutions, the primary responsibility for cybersecurity lies with the customer or their chosen reseller partner. While VMS solutions can be configured securely, it is ultimately the customer's or partner's technical team that must ensure a proper implementation of the system. Regrettably, many on-premises customers lack awareness of their system's security needs, presenting a significant challenge.

Some common vulnerabilities that pose cyber threats to on-premises solutions include:

- Outdated software
- Weak passwords
- Insecure network connections
- Misconfigured or missing encryption

A widespread misconception prevails that offline systems, with no public access, are inherently secure. However, the reality is far more intricate. Configuring network connections securely can be technically demanding, especially for smaller customers without a dedicated IT department or those reliant on their physical security team. As physical security and IT converge, a comprehensive understanding of both disciplines becomes increasingly crucial.

Even with a secure system in place, an incorrect installation can undermine its advantages. Given the pivotal role of cybersecurity in the modern IT landscape, technical competency is an absolute necessity for every on-premises customer. Some common vulnerabilities that pose cyber threats to on-premises solutions include:

Cloud

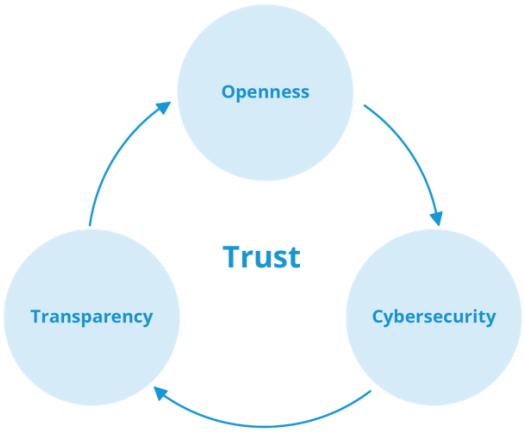
Cloud-based surveillance solutions transfer most of the responsibility for security to the vendor. In cloud terms, this is known as the 'Shared Responsibility Model', both parties take their share of the responsibility for security. For Surveillance as a Service (SaaS) solutions, most of the responsibility for security falls on the vendor, however, the customer is still responsible for configuring who has access to the service so that it is secure. Typically cloud vendors offer sophisticated encryption options, both for transmission (data-in-transit), and for storage (data-at-rest), but again it is the customer's responsibility to ensure these are configured correctly. Some common vulnerabilities that pose cyber threats to cloud solutions include:

- Misconfiguration, the service is not configured securely at the customer's site
- Weak password practices
- Vulnerabilities in the interface's security

Selecting a reliable cloud solution goes beyond brand recognition, before deciding, ask yourself: Can the vendor be trusted with your data? Are they reliable? Do they have robust technical procedures in place to ensure video data security? Prioritizing vendors committed to security and transparency and recognizing the significance of technical expertise in cybersecurity can greatly influence your decision-making process

Openness and transparency

Openness and transparency regarding vulnerabilities are crucial when it comes to safeguarding your video technology solution from cyber attackers. This requires a continuous collaborative effort between you and your vendor.



Leading industry players like Microsoft and Google set a high standard in this regard. Their transparent security practices foster strong customer trust. If a vendor you are considering hesitates to address your security concerns, take it as a potential red flag.

As a customer, it is essential to be aware of any weaknesses in the vendor's system. Vendors must demonstrate honesty by openly acknowledging vulnerabilities and detailing their security measures. By being upfront about weaknesses, vendors enable customers to take proactive steps to mitigate any risks.

Conversely, any lack of transparency can lead to challenging situations. If a vendor is aware of a weakness but fails to inform their customers, and the weakness is exploited by malicious actors, the vendor finds themselves in a precarious position. Full transparency is of utmost importance in the relationship between vendors and customers. Customers need to be able to trust vendors to be fully open about the security of their system, both its strengths and weaknesses.

Responsible vulnerability disclosure

Responsible disclosure empowers customers with accurate information to make informed decisions and effectively secure their systems. Given that every software has vulnerabilities, the failure to openly disclose them indicates a lack of willingness to share potential issues with customers, which is concerning. However, this can also be a double-edged sword, as providing too much detail about vulnerabilities may inadvertently aid hackers in exploiting them.

It is important to verify if the vendor follows strict disclosure policies in compliance with relevant standards to ensure the best cybersecurity experience. Additionally, it is crucial to inquire about their vulnerability handling process, which should encompass security investigation, mitigation, and disclosure. It is vital that the vendor provides prompt and free software updates for any identified vulnerabilities. Lastly, it is worth verifying that the vendor actively encourages security researchers, customers, and partners to report any potential security vulnerabilities related to their products.

The human factor - a weak link in security

It is important to acknowledge that achieving a 100% secure system is a challenging task. As with most situations, when humans are involved, there is always a potential security risk. Someone, either willingly or unwillingly may compromise the system, Therefore, the human factor is often considered a weak link in security. Education and training play a critical role, both to ensure the solution is used correctly, and customers apply all necessary security patches.

Occasionally, humans express reluctance towards enhanced cybersecurity measures because they see them as making the solution more complex and difficult to use. However, it is crucial to strike a balance between security and usability. While security does come with a price, it is a price worth paying.

Security for video technology is not a luxury, but a necessity in this digital age. Be proactive, apply all recommended security patches, and ensure your systems are up to date.

Milestone Systems is a leading provider of data-driven video technology software in and beyond security that helps the world see how to ensure safety, protect assets, and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 500,000 customer sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.