SECURITHINGS

The Latest Trends in Managing Physical Security Devices

Complexity, Trends, and the Shift to Automated Solutions

A Data-Focused Look at the Growing Need to Automate the Management of Physical Security Devices

As the usage of physical security devices has grown in recent years, the ecosystems in which these devices operate have become more complex. Not only have the sizes of fleets of physical security devices increased, but it is common for them to include a variety of device types, such as cameras, access panels, intercoms, turnstile gates, digital signage devices, network extenders, intrusion detection devices, and others. And for each kind of device, it is common for organizations to have numerous models, which were produced by different manufacturers and run different firmware, often managed in silos including different management systems.

Considering that the performance and security of each device is affected by many external factors, it makes sense that managing these devices has become an increasingly difficult task. As a result, recent years have seen a growing awareness of the difficulties, expenses, and risks that plague organizations that try to manage their physical security devices manually (or that fail to manage these devices at all).

How significant are the problems facing organizations that have not yet begun to automate their approach to managing physical security devices? We at SecuriThings have gathered key data to answer that question from several large organizations. Since these are organizations that until recently managed their physical security devices manually, our work with them has provided us with valuable insights into the challenges they previously faced due to the growing complexity of managing a typical fleet of physical security devices.

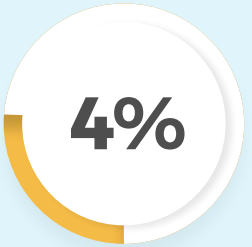
Using exclusive information gathered by our teams, this report will provide an inside look at our key findings. In addition to exploring the complex challenge of managing entire fleets of physical security devices, the following pages will assess the scope of the problems facing organizations that manage their physical security devices manually.

By the Numbers: How Serious Are the Problems Facing Physical Security Devices?

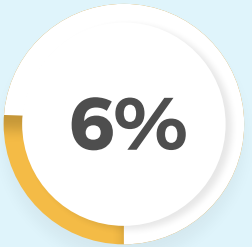
Perhaps the clearest evidence of what is at stake for organizations struggling to adequately manage their physical security devices is found in the frequency with which these devices go offline and the operational issues they face.

With many of these devices having multiple issues, 26% of these devices have at least one operational issue that needs to be addressed. These issues included (among others):

- Outdated firmware
- Security vulnerabilities
- Weak passwords
- Poor configuration



Our data has shown that over the course of an average week, 4% of physical security devices got completely disconnected from their network for some amount of time.



Meanwhile 6% of devices were completely disconnected from their video management system.

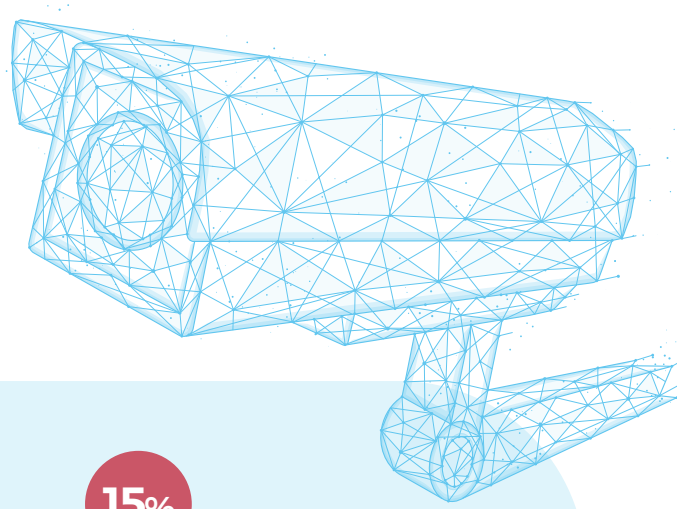
In addition, many of these devices had reached their end of life, leaving them with no way to get new firmware upgrades and support from the manufacturer.

Drilling down into this data showed that 9.4% of physical security devices had at least one cybersecurity vulnerability, each of which heightened its organization's exposure to the risk of a cyberattack.

Our data also showed that more than 70% of devices were running outdated firmware. Manually upgrading firmware for a fleet of diverse devices can be a time-consuming and inefficient process, but in some cases outdated firmware can lead to erratic functioning and even malfunctions that can force a device offline. And, because firmware upgrades often include necessary patches, a failure to install them often leaves an organization's physical security devices with unpatched cybersecurity vulnerabilities.

In addition, we found that 8% of devices were misconfigured. In many cases, misconfigured devices expose the organization to cybersecurity vulnerabilities.

Finally, 15% of physical security devices were no longer supported, because they had passed their end of life, while 40% were scheduled to reach their end of life within three years.



Threats by Numbers

9.4%
Found to have cybersecurity vulnerabilities

70%
Of devices were found to be running outdated firmware

8%
Of devices were misconfigured

15%
Of devices were no longer supported

How the Growing Complexity of Managing Physical Security Devices Fuels These Issues

The complexity of managing physical security devices is a major factor in the frequency of device downtime and issues such as outdated firmware, cybersecurity vulnerabilities, weak passwords, and poor configuration settings. Without an adequate solution for addressing that complexity, many organizations fail to promptly notice and manage the specific issues that affect their physical security devices.

The complexity of managing physical security devices results in issues such as:

- Outdated firmware
- Cybersecurity vulnerabilities
- Weak passwords
- Poor configuration settings

One key factor in that complexity is the breadth of factors that affect the operational status of each physical security device.

The performance of each of these devices depends not just on its own health, but also on the health of the surrounding ecosystem, including elements such as network components, switches, gateways, power sources, and more. Accordingly, our findings showed that the most common causes of device downtime included network issues, disconnection from video management systems (VMS), power outages, high usage of CPU power or RAM, and extremely high or low temperatures.

That makes it important to monitor the entire ecosystem surrounding a fleet of physical security devices as comprehensively as possible, both to keep tabs on the operational status of each device and to diagnose and resolve any issue that comes up.

Meanwhile, the variety of physical security devices in a typical fleet makes managing those devices a particularly cumbersome task. Although security cameras are the most common type of digital device used for physical security, they are far from the only type of device often used in organizations' fleets. And for any type of device, a fleet could include multiple models from various manufacturers that run different software, have different issues, and require different maintenance steps to be taken at different times.

Also adding to the complexity of managing physical security devices is the simple fact that their deployments are growing as their usage spreads. Over the course of 2021, the aggregated data we collected showed a 10% year-over-year increase in the number of physical security devices being used by an average customer—indicating a notable rise in the volume of devices to be managed.

No less importantly, many organizations suffer from an organizational structure that exacerbates the complexity of their deployments. It is common for multiple stakeholders to be involved in managing these devices—often including in-house physical security and IT departments, alongside third-party systems integrators and sometimes other team members. Lacking an owner to oversee all aspects of device management often creates both inefficiency and a risk that problems will "fall through the cracks" between various teams.

> **We noted a 10% year-over-year increase in the number of physical security devices being used by an average enterprise**

Top reasons for downtime:

- Network issues
- Disconnection from management systems
- Power outages
- High usage of CPU power or RAM
- Extremely high or low temperatures

A Major Blind Spot for Many Organizations—and Why It Matters

Perhaps the single greatest factor contributing to the challenge of managing physical security devices is most organizations' lack of real-time visibility and control regarding the operational status of their devices. Because this **makes it difficult to know whether a given device is working properly at any given time**, organizations' physical security teams typically take a reactive, manual approach to determining when a device has gone offline.

Furthermore, even when a company does discover that there is an issue with one or more of its devices, the process of manually identifying and resolving the issue is typically inefficient. Without remote access to real-time data, even simply diagnosing an issue often requires a **costly truck roll** so that a technician can inspect the device and its environment in person.

As a result, the process of handling issues that affect devices generally requires coordination between IT and physical security teams (as well as systems integrators in some cases). The amount of time-consuming communication and in-person work involved in this process makes it particularly expensive. Most importantly, this situation increases the **risk that one or more of an organization's devices will go offline for an extended period** before the organization manages to discover, diagnose, and resolve the issue.

Exacerbating these difficulties, many organizations fail to consistently take routine maintenance steps such as rotating their devices' passwords or upgrading their firmware. Organizations lack an automated system to make sure such steps are taken whenever required, and they do not invest the necessary resources to adequately perform routine maintenance manually. This situation creates both operational and cybersecurity risks—especially given the **growing risk of cybercrime** seen in recent years.

While some organizations have not yet realized that managing physical security devices manually is risky and inefficient, others recognize these problems but are not sure how to address them. On the other hand, an increasing number of organizations do understand the value of automating the operational management of devices.

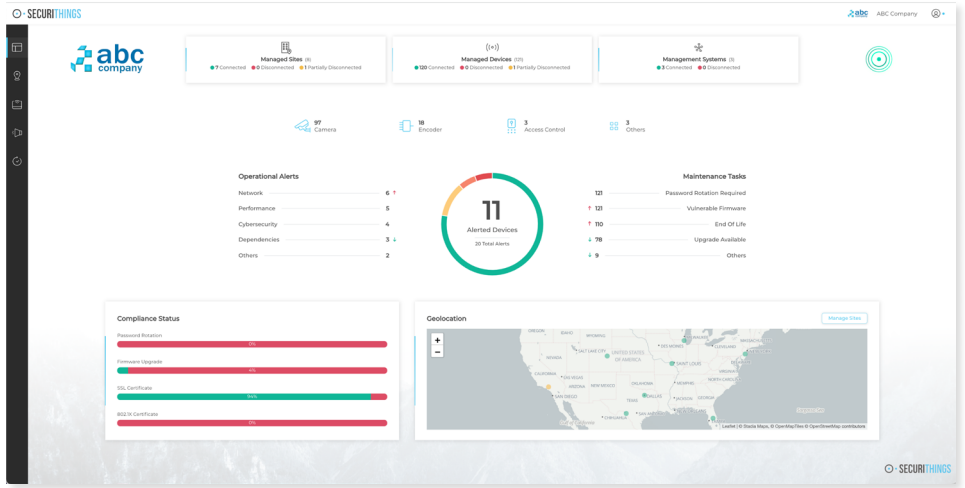
It's difficult to know whether a particular device is working properly at any given time

IoTOps: Addressing These Challenges Through Automation

Whereas today most organizations have a reactive approach to managing their physical security devices, a shift towards more effective ways of managing these devices has already begun.

Some organizations have taken steps in this direction by simply adding more predictive and preventive elements to their management of physical security devices. But for the organizations most determined to maximize the benefit they see from their devices, there is no substitute for a comprehensively automated approach to managing them.

The key to bringing the power of automation is **IoTOps—a practice that allows for the operational management of physical security devices to take place in a consolidated, automated, and secure manner**.



While providing real-time visibility into the operational status and health of physical security devices, IoTOps enables physical security and IT teams to automate the security, operations, and predictive maintenance of these devices. IoTOps also addresses the gaps between the various stakeholders often involved in managing physical security devices. Not only does it bring IT standards to the realm of physical security, but it involves automatically alerting the most relevant team members when a physical security device faces an expected or unexpected issue.

How Does IoTOps Offer Concrete Business Benefits to Today's Organizations?

By alerting organizations in real time when a physical security device goes offline, IoTOps helps them improve their system availability.

By minimizing the need for expensive manual work (especially on-site work), IoTOps helps organizations reduce their costs.

By standardizing routine maintenance steps, IoTOps helps organizations ensure compliance with relevant laws and their own policies.

By monitoring devices and alerting team members to any anomalies that appear, IoTOps helps organizations protect themselves from cyber threats.

By providing advance notice of issues expected to face physical security devices in the near future (including a device's end of life), IoTOps gives organizations useful visibility for future planning.

Benefits of an Automation-Focused Approach

In light of those benefits and the growing challenge of managing physical security devices, it is not hard to see why organizations are choosing this approach.

Today's organizations are becoming increasingly reliant on digital devices for physical security, even as they also become more aware of the challenges that those devices present. As more of these organizations see the benefits of using automated technologies such as our Horizon solution, they will understand the importance of adopting the principles of IotOps—namely, to consolidate, automate, and secure their approach to managing physical security devices.

Not only will this shift allow them to manage their physical security devices more efficiently and reliably, but it will empower these organizations to maximize the benefits—and ultimately the ROI—provided by their physical security devices.

SECURITHINGS

ABOUT SECURITHINGS

Founded by leading security and IoT experts, SecuriThings empowers Operations & IT professionals to automate the operational management of IoT devices at scale, while also ensuring full compliance and security within their organization. The solution is trusted by Fortune 100 companies and has been deployed by numerous large enterprises such as major airports, universities, hospitals and more. SecuriThings partners with key system integrators as well as device manufacturers to provide unprecedented insights, coverage, and reliability.

For more information, please contact us at **info@securithings.com.**

www.securithings.com