Connected Device Security and Vulnerability Management for Hospitality

Hospitality organizations including hotels and casinos rely on a broad range of connected technologies to provide a seamless guest experience. From check-in kiosks and digital keycards to automated lights, temperature sensors, and minibars, Internet of Things (IoT) technology is essential to operations.

However, historically, the hospitality industry was slow to adapt to the realities of modern cybercrime. Many hospitality organizations took a long time to recognize the importance of a robust cybersecurity program—and, as a consequence, became enticing targets for cybercriminals.

The average cost of a hospitality data breach in 2023 was $3.36 million, up from $2.94 million in 2022. That's a 14% increase in the space of a year. At the same time, where hospitality accounted for just 2% of data breaches in 2019, it now accounts for 4%.That may not sound like much… but it represents a massive increase in attacks worldwide.

A recent report found that almost a third (31%) of hospitality organizations have reported a data breach in their lifetime. Of those, 89% had been affected more than once in a year.

IoT Risks for Hospitality

IoT devices are often insecure. They come with default passwords that are easy to guess and difficult to change before connecting to the internet. Their firmware is often built with speed to market instead of security at the forefront. Further, the reality that IoT devices lack agreed-upon security standards means that device manufacturers have no real best practices to adhere to. This creates what amounts to thousands of potentially insecure devices out in the real world. Even without the basic lack of security in IoT devices, however, cybercriminals still find the hospitality sector a target-rich environment.

Top IoT Security Challenges

- Growing Attack Surface
- Connected Supply Chains
- Legacy Systems and Equipment
- Accurate IoT Inventories
- Third-party Security Standards
- Regulatory Compliance

Recent Attacks on Hotels and Casinos and the Consequences

Attacks in the industry are near-universally financially motivated, with the majority aiming to steal information that can either be sold or used to make a profit. Credit card information is a primary target, but cybercriminals also aim to steal sensitive guest information to commit fraud and use it as leverage for ransom demands.

The 2023 Data Breach Investigations Report identified malware (e.g., ransomware and RAM scrapers), web application attacks, and social engineering as the most significant threats to hospitality organizations.

One of the major causes of cybersecurity risk in hospitality is the high prevalence of connected devices—everything from online booking systems and digital keycards to automated lights, temperature sensors, minibars, and more.

Similarly, casinos have started to experience cyberattacks as they shift more of their operations to digital platforms. A shift to connected devices including internet-enabled slot machines and internet-connected security cameras opens up new fronts for threat actors to exploit. In fact, the attack that brought down MGM originally intended to rig the casino's slot machines.

Cybercriminals are targeting the money-rich environment casinos have created. The addition of numerous Internet of Things (IoT) devices into the modern gaming facility – including IoT security cameras, slot machines, fish tank thermometers, and more – means that casinos have a vast network and attack surface with many options for cybercriminals.

In 2017, in one of the classic IoT security hacks, a casino was breached because of an IoT thermometer in a fish tank.

The broad use of connected devices opens up casinos to the game of chance that an attacker could breach them and steal customer data or other information. So casinos remain a target, but not for the cash they have on hand in vaults like in Ocean's 11. Rather, the new money is data and cybercriminals are looking.

A few recent attacks on hotels and casinos include:

- In mid-2023, MGM Resorts International reported a massive cyberattack that resulted in over $100 million in costs and the theft of an unspecified amount of personal guest information. MGM Resorts stated hotel occupancy fell to 88% during September (compared to 93% the previous year) largely as a result of the attack disrupting the company's website and mobile applications used for reservation

- Motel One, a budget hotel chain operating in Europe and the U.S., was hacked in late 2023 by cybercrime group AlphV/BlackCat. The company's primary strategy appears to have been to downplay the incident—however, the fact remains that a considerable amount of personal data was stolen, and there is no doubt the incident will have been costly and embarrassing for Motel One.

- In September 2023, Caesars Entertainment confirmed a major breach in which attackers stole the company's loyalty program database—the largest of its kind in the industry. The database contains highly personal information, including driver's license details and social security numbers. Beyond the $15 million ransom payment, this incident has had a significant financial impact for Caesars Entertainment. The full scope of the costs including remediation and investigation of this incident has not been determined.

Unmanaged IoT Devices Leads to Increased Attack Surface and Risk

Shadow IT is one of the most persistent cybersecurity challenges today. Already, researchers estimate that 53% of departments refuse to use IT-approved tools and 80% of workers admit to using SaaS applications at work without getting approval from the IT department.

Connected devices often have at least a network interface, like ethernet, Bluetooth, Long-Term Evolution (LTE), Zigbee, Wi-Fi, 5G, or Ultra-Wideband (UWB). Once deployed in a network using these connection methods, IoT systems can be readily discovered and connected to the open internet. This is a major issue because they're not designed to have any setup protocols before connecting to the internet.

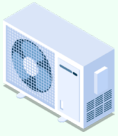
Once threat actors gain initial access into a network from a discoverable IoT device, they're able to laterally move deeper into the information architecture to achieve their goals. At the individual device level, IoT equipment is particularly vulnerable to common security pitfalls.

In terms of which categories of connected devices organizations tended to buy, Keyfactor research found that companies tended to deploy the following IoT solutions:

Hybrid work technologies	53%
Security cameras	53%
Real-time monitoring and location tracking	52%
Inventory and asset management	46%
Door locks or physical security	43%
Smart lighting	40%
Space utilization technology/tools	38%
Air quality monitoring	35%

Common Unmanaged IoT Devices

Sensors


HVAC

Guest Room Automation

Routers

Delivery Robots

Meters and Sensors

Automated Check-in

Door Locks

Printers & Scanners

Displays

Alarms

Badge Readers

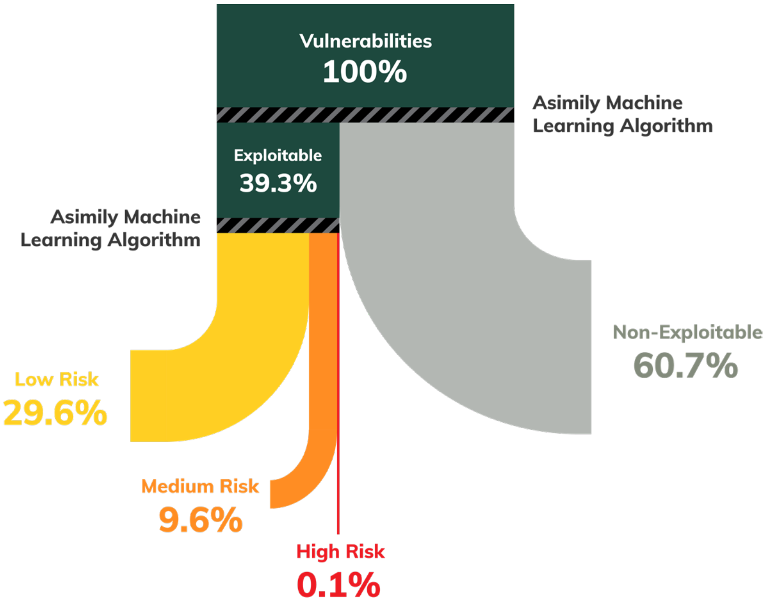
Security Cameras

Inspection Sensors

Secure Your Connected IoT Devices and Reduce Vulnerabilities 10x Faster with Half the Resources

Your reputation depends on timeliness and avoiding delays. When threats are kept out, everything stays on time and business can grow. Asimily IoT security solutions help you ensure that outside attackers don't affect your operations.

Asimily empowers vulnerability management teams to tackle the riskiest issues first. Instead of just giving you a list of vulnerabilities to fix, Asimily combines that information with unique Impact and Likelihood analyses to get a risk-ranked set of devices whose vulnerabilities can be mitigated.



Accurate Inventory & Unmatched Visibility

Harness Asimily's powerful protocol analyzer and deep packet inspection (DPI) to safely discover and automatically categorize your IoT assets, services, connections, and apps giving you the power to proactively manage risks, optimize resources, and fortify your security like never before.

Vulnerability Prioritization & Efficient Mitigation

Asimily's unique Impact, Likelihood and Utilization analyses show which vulnerabilities attackers will take advantage of in your environment. Allocate your resources to the riskiest devices first to promptly address vulnerabilities.

Threat Detection & Incident Response

Set device behavior rules that instantly identify any suspicious activities. Our engine swiftly spots deviations from normal behavior, ensuring that you can respond promptly to potential threats. Detect misconfigurations as well, keeping security posture high.

Risk Modeling & Simulations

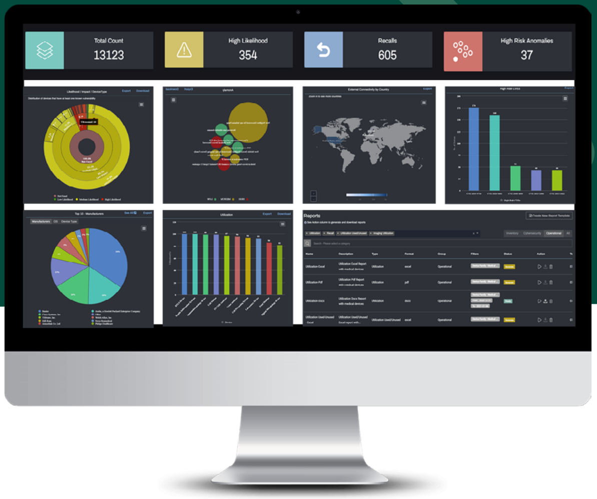
Envision, predict, and act with unparalleled confidence, and unlock a new era of proactive risk mitigation. Calculate the least risk associated with a device before configuration and connection.

Connected Device Security, Reimagined

Securing the Internet of Things is far more complex than securing traditional IT equipment. Poor security practices at IoT device manufacturers paired with minimal visibility by IT and security teams make connected equipment a major security risk. The distributed and broadly installed nature of these devices means that a risk-based approach is required. This can be done, and thankfully Asimily can help companies implement and manage a risk-focused method of securing IoT devices for a more secure future.

Asimily's IoT Risk Management Platform

- Creates a complete IoT inventory, collecting 100+ attributes for each device;
- Identifies and prioritizes the riskiest vulnerabilities;
- Recommends simple, validated mitigation actions;
- Conducts a full flow analysis for each device, recording all communication patterns across the network;
- Calculates risk for every connected device based on device attributes, dataflows, vulnerabilities, anomalies, configuration, and overall criticality of the device on operations;
- Generates ACLs for targeted segmentation for use by a NAC;
- Flags anomalous device behavior based on profiling data from millions of IoT devices;
- Makes it easy to set policies to monitor accepted risks and identify suspicious activity proactively;
- Automates packet capture for forensic analysis of any IoT device to support root cause analysis;
- Documents when the device is being used so users can understand utilization and operational efficiency;
- Allows device configuration snapshots to be taken, to thwart ransomware and simply recovery; and
- Risk simulator helps determine the benefit of work before it is performed, increasing team efficiency.



Name	Description	Type	Format	Group	Filters	Status	Action
Utilization-Excel	Utilization Excel Report with medical devices	Utilization	excel	Operational	[illegible]	[illegible]	
Utilization-Pdf	Utilization Pdf Report with medical devices	Utilization	pdf	Operational	[illegible]	[illegible]	
Utilization-Docx	Utilization Docx Report with medical devices	Utilization	docx	Operational	[illegible]	[illegible]	
Utilization Used-Unused - Excel	Utilization Used/Unused Excel report with...	Utilization Used/Unused	excel	Operational	[illegible]	[illegible]	

Asimily can help enterprise organizations drastically reduce cyber risk while minimizing resource and time costs.

To see how Asimily can help your organization, **arrange a demo today.**

About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, pharmaceutical, and enterprise companies.

Connect With Us

info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY