Connected Device Security and Vulnerability Management for the Government and Public Sector

Government and public sector organizations are exposed to more and more sophisticated cyberattacks than any other sector. Compared with the first quarter of 2023, cyberattacks against government agencies and public sector services rose 40% in the second quarter of 2023, according to Blackberry's second Quarterly Threat Intelligence Report. Attacks on government and public entities ranked among the top four.

Government and public sector organizations differ from private-sector organizations in many ways. Some—such as local governments—perform a far greater number of functions than any private-sector organization, making them extremely complex entities with technology profiles to match.

The recent Data Breach Investigations Report (DBIR) identified system intrusion (hacking), lost and stolen assets, and social engineering as the most prevalent threats to government organizations. These threats are consistent with the fact that attackers are often seeking more than profit—government and public sector organizations often hold highly valuable and sensitive data, and threat actors will often go to extreme lengths to obtain it.

And then there's cost. The 2023 Cost of a Data Breach study found that government organizations spent an average of $2.6 million to recover from a data breach in 2023—an increase of over 25% from $2.07 million in 2022.

IoT Risks for Government and Public Organizations

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 government and public 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 Government and Public Sector and the Consequences

Government and public organizations have large and complex attack surfaces. Naturally, this makes security a constant challenge and provides attackers with a much broader range of options when it comes to choosing targets and attack vectors.

One major cause of cybersecurity risk in the government and public sector is the high prevalence of connected devices and IT systems—everything from online registration systems and smart cities to staff-owned mobile devices, vehicle trackers, and more.

Government and public organizations are targeted by a broader range of potential attackers compared to the private sector. According to the DBIR, roughly 30% of attacks against public sector targets are motivated by espionage, 2% are ideological, and the remaining 68% are financially motivated. As you'd expect, the tactics and techniques used in each of these categories vary significantly, creating further difficulties for cyber defenders

Corvus Insurance analyzes ransomware leak sites (dark web sites where ransomware groups post stolen data) to track evolving trends. There was a 95% increase in ransomware attacks in government agencies and law practices in Q3 of 2023, according to the recent Corvus report. A common form of ransomware, LockBit, tripled its government victims between Q2 and Q3, primarily affecting municipalities and cities.

Malicious actors can attack government databases to obtain strategic information — for example, Russian state-sponsored hackers breached US defense contractors and stole military and communication infrastructure data from at least January 2020, through February 2022. In 2023, several US federal government agencies have also been hit by Russian cybercriminals. Some breaches can reveal the personally identifiable information of government officials. For instance, the Pentagon has reported that 26,000 individuals were affected by email data breaches in 2023.

Governments can not afford to underfund cybersecurity efforts, in an era of constant threats. With agencies facing regular operational disruptions, resilience has become a critical enabler of mission success. And this increasingly clear link has elevated resilience to the top of the government's priority list.

A few of the most recent attacks on government and public sector organizations include:

- In February 2023, the City of Oakland, California, declared a state of emergency after a ransomware attack. Essential services such as 911 were unaffected; however, many non-emergency systems were taken offline while the City's IT department worked to resolve the incident, and some government buildings were forced to close temporarily.
- In mid-2023, the UK Electoral Commission publicly disclosed that it had been targeted by a "complex cyberattack." The attack resulted in the theft of 40M personal data records relating to everyone in the UK who registered to vote between 2014 and 2022—roughly 86% of all British adults as of 2022.
- Chinese hackers covertly accessed email accounts belonging to individuals at over two dozen U.S. organizations, including at least two U.S. Government agencies—the State and Commerce Departments. Official government statements put the number of affected agencies "in the single digits."
- A massive attack campaign conducted by Russian cybercrime group Clop in mid-2023 targeted organizations worldwide that were customers of Progress Software. Victims included large enterprises and government agencies worldwide, including multiple U.S. state governments and federal agencies.

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.

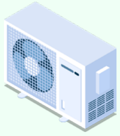
Connected devices often have at least a network interface, like ethernet, Bluetooth, Long-Term Evolution (LTE), Zigbee, Wi-Fi, 5G, or Ultra-Wideband (UWB). Once deployed in a network using these connection methods, IoT systems can be readily discovered and connected to the open internet. This is a major 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.

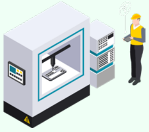
In terms of which categories of connected devices organizations tended to buy, Keyfactor research found that companies tended to deploy the following IoT solutions:

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


HVAC

Sensors


Equipment

Routers

Smart Energy Meters

Workstations

Drones

Printers & Scanners

TVs

Alarms

Badge Readers

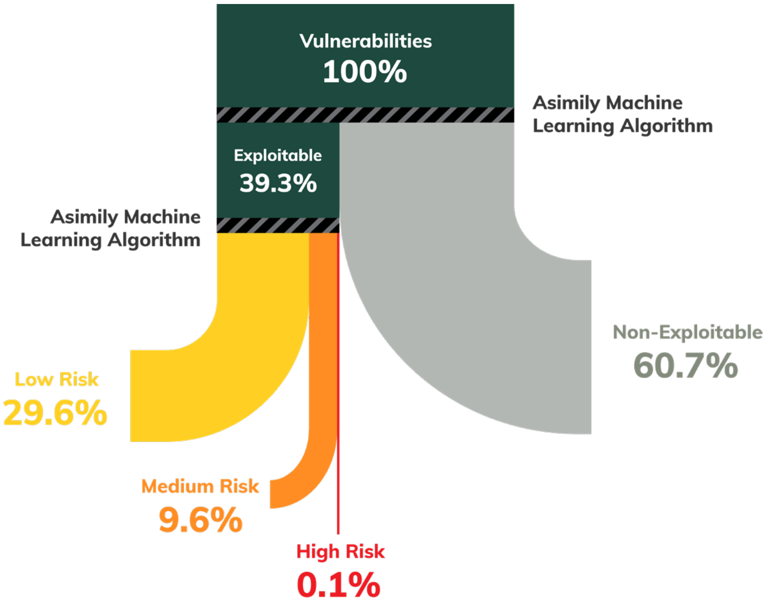
Security Cameras

Autonomous Vehicles

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.

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