

IoT Device Security in 2024: The High Cost of Doing Nothing

Protecting the Growing IoT
Architecture in a Complicated
Security Environment





Table of Contents

Introduction	3
Unmanaged IoT Devices Leads to Increased Attack Surface and Risk	4
Most Common IoT Security Challenges	5
Most Commonly Targeted IoT Devices	6
Cybercriminal Tactics Targeting IoT	7
The High Cost of Doing Nothing	8
Cyber Insurance is Not Enough	10
IoT Security Predictions for 2024	12
The Most Targeted Industries in the Past 12 Months	14
Recent Attacks on Manufacturing and the Consequences	15
Recent Attacks on Healthcare and the Consequences	16
Recent Attacks on Gaming and Casinos and the Consequences	17
Recent Attacks on Higher Education and the Consequences	18
Recent Attacks on Transportation and Logistics and the Consequences	19
Recent Attacks on Life Sciences and the Consequences	20
Recent Attacks on Utilities and Critical Infrastructure and the Consequences	21
A Holistic Approach to IoT Security	23
How Asimily's Patented Remediation Compares to the Traditional Approach	24
Develop Baseline Risk KPIs	25
Managing and Mitigating IoT Vulnerabilities	26
Effectively Incident Response & Forensic Analysis	28
Recover from Configuration Drift, Ransomware & More	29
Integrations Are Crucial for Better Risk Reduction	30
Evaluate Risk Before Moving Forward	31
Asking for Budget	31
Asimily Can Help	32

IoT-related cyberattacks hit every industry. Understand the risks and how to mitigate them with the insights in this report.

IoT devices are uniquely vulnerable in the face of the rising tide of cyberattacks as modern enterprises rely on connected devices to improve efficiency and operational performance.

The Internet of Things (IoT) is becoming larger every year. [According to IoT Analytics](#) data, the number of connected devices online worldwide is expected to surpass 29 billion by 2027, a sharp increase from 16.7 billion sensors in 2023. This means more devices coming online and accessible from anywhere in the world.

This flood of new interconnected devices can make a big difference in modern business. Warehouses can monitor inventory levels. Life sciences firms can control temperature in laboratories. Manufacturers can monitor production lines from remote locations. Utilities can track water quality without needing to go on-site. Transportation and logistics providers can track the real-time positions of ships, trains, or trucks.

These individual connected devices have a bevy of uses throughout the modern world, in business, healthcare, and consumers' day-to-day lives. The cornucopia of use cases has meant that people can measure and monitor more than they ever could more easily than before.

Securing traditional endpoints – computer workstations, servers, etc. – while not necessarily ever easy is at least a more clear-cut strategy. These traditional computer systems allow for extensive security to be applied before they're ever connected to the internet. IoT devices instead connect to the internet automatically once they're turned on. These "other endpoints" are growing in volume far faster than traditional information technology. This creates a huge problem because IoT devices explode the average corporate attack surface in size and scope.

With all the weaknesses and none of the defensibility of standard targets like servers and workstations, the Internet of Things creates a security challenge that is unparalleled in the modern age. Put simply, using



connected devices puts companies at higher risk of a data breach. However, as the saying goes, the cat is already out of the bag. IoT devices will be used more and more in the coming years, and cybersecurity teams need to be comfortable with how to best defend against an attack coming from their IoT infrastructure.

This guidebook can provide a baseline for understanding the challenge of securing the Internet of Things, while also offering key guidance for businesses seeking to develop an effective defensive strategy. Over the course of this report, you will learn about:

 **The Emerging IoT Device Security Trends and Challenges**

 **The Most Targeted Industries and Recent Attacks**

 **The High Cost of Doing Nothing**

 **Why Cyber Insurance Isn't an Effective Backstop**

 **IoT Predictions for the Next Three Years**

 **A Holistic Approach to Reducing the Risk of a Cyberattack Succeeding**

Unmanaged IoT Devices Leads to Increased Attack Surface and Risk



As IoT devices become more popular and more broadly deployed, there are a few challenges to be aware of with respect to their overall security. IoT devices are not always designed with security in mind. Traditional IT systems commonly come preloaded with security technology designed to offer a base level of protection. Most of these systems also require a setup process before they can be used, which allows them to download updates to secure them against at least known attacks.

There are also some standards in place for how to build traditional IT equipment to ensure security. This isn't the case with the Internet of Things. The creators of IoT operating systems and devices have no accepted industry standard for security, and yet 80% of companies have [integrated IoT into their operations in some way](#). These devices could be in any number of situations, including environment sensors in factories, connected medical devices in hospitals, and smart TVs or whiteboards in corporate conference rooms. They're also often built with low-cost, outdated software and deprecated hardware. The lack of standardization leads to a swath of heterogeneous software and hardware that may have conflicting systems and further complicate securing them.

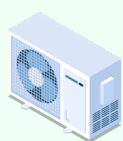
Connected devices often have at least a network interface, like ethernet, Bluetooth, Long-Term Evolution (LTE), Zigbee, Wi-Fi, 5G, or Ultra-Wideband (UWB). Once deployed in a network using these connection methods, IoT systems can be readily discovered and connected to the open internet. This is a major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

IoT devices might have hard-coded default passwords, which are often difficult to update. For example, CVE-2021-45522 notes that [NETGEAR XR1000 devices before 1.0.0.58](#) have a hard-coded password that can't be changed. Moreover, it's easy to find commonly used IoT passwords online. Default passwords open up the network to attacks because it's easy for threat actors to use them for initial access. When used at scale, attackers can use weak IoT passwords to provide an easy foothold into the network. IoT devices are shipped and deployed at an unprecedented scale, which makes updating the password quickly enough nearly impossible. That's if there is an accessible UI that makes it possible to change the default password in the first place, and the default password isn't included in the device's firmware.

To make matters worse, many IoT devices lack vendor support for patching vulnerabilities. Vendors either don't release patches for their devices, or the devices won't accept patches without breaking down. Many IoT products aren't designed to be easily updated or can't be taken offline because they're too critical. Implantable devices fit this description, as do sensors in nuclear power plants.

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. Even one unprotected device can lead to a potentially damaging attack. These challenges need to be addressed to account for rising attacks on IoT devices, especially among some of the most commonly targeted assets.

Common Unmanaged IoT Devices



HVAC



Sensors



Equipment



Routers



Smart Energy Meters



Manufacturing Workstations



Drones



Printers & Scanners



TVs



Alarms



Badge Readers

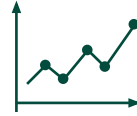


Security Cameras



Autonomous Vehicles

Most Common IoT Security Challenges



IoT devices add a new dimension to the challenges cybersecurity teams face. Securing enterprise infrastructure is difficult at the best of times. [According to a 2023 report from IBM](#), it takes 207 days on average to identify a data breach. Once a breach is identified, [that same study](#) found it would cost an average of \$4.45 million in direct costs – the highest number ever recorded. This number doesn't include any long-term impacts of lost revenue from reduced staff focus or reputational damage.

Ransomware attacks globally show no sign of stopping. In one year, there were more than [1,900 documented ransomware attacks](#) against the United States, Germany, France, and the United Kingdom. The report from Malwarebytes showed that the United States experienced 43% of those attacks, while the number of ransomware attacks in France nearly doubled in the last five months. These attacks are getting more expensive as well. According to [SC Magazine](#), the average ransomware payout increased from \$812,380 in 2022 to \$1,542,333 in 2023.

Securing connected devices in this environment is fraught with challenges. This is true for several reasons, not least of which is the sheer scale of connected devices that come online at any given time. IoT equipment tends to be deployed en masse in an organization. That many devices connecting to the corporate network – no matter where it is – at any given time strains even the most put-together security teams.

98%

of IoT traffic remains unencrypted

It doesn't help that many IoT device manufacturers haven't prioritized security in their products. They might build the device with no data encryption in place, or make it impossible to update the device's software to a new version without the device breaking.

In fact, [98% of IoT traffic](#) remains unencrypted. Such a lack of even baseline data encryption in IoT makes any personal and confidential data easy to access from the open internet.

There's also more IoT-specific malware in play as cybercriminals have noticed how easy it is to breach these devices. For instance, [Zscaler identified](#) a 400% increase in IoT malware in a single year. Threat actors have noticed the weaknesses in connected devices if the increase in malware targeting those systems is any indication.

The rise in IoT malware makes it vital that enterprises focus on securing their connected devices. So it's concerning that [55% of companies](#) don't require third-party IoT providers to comply with security and privacy measures and 56% don't keep an inventory of IoT devices. Coupled with the rise of IoT-specific malware, the increase in ransomware more generally, and the lack of effective defenses for connected devices, organizations using IoT systems need to be more cognizant of the risks. The next twelve months will see some changes in the IoT security landscape, and we anticipate a few changes in terms of protecting connected devices.



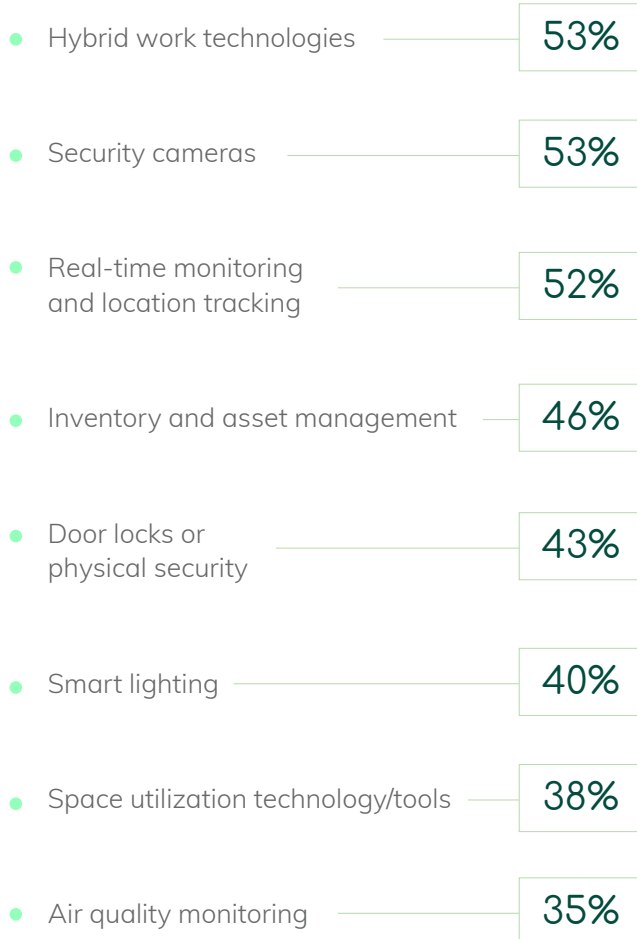
Most Commonly Targeted IoT Devices



Not all IoT devices are targeted at the same rate. Among the different types of IoT equipment deployed in the enterprise, some are more commonly the target of attacks. Routers and other network devices are among these, as are security cameras, IP cameras, digital signage, media players, digital video recorders, printers, and smart lighting. Many of these are highly vulnerable to cyberattacks.

For example, routers are among the most targeted devices in the enterprise. [Recent research](#) showed that routers accounted for 75% of IoT infections, with connected cameras accounting for 15%. This is understandable, as routers commonly allow for connections to other devices within the network and can be used as a launching pad for lateral movement.

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



These categories of commonly used IoT devices ignore the specialized equipment used in healthcare settings. Health delivery organizations like hospitals also deploy nuclear medicine equipment, blood glucose monitors, internet-connected pacemakers, and other medical devices designed for patient and in-hospital use.

In addition to specialized connected medical devices, there are different IoT devices in use throughout enterprises. Real-time monitoring might include temperature sensors in factories or water quality equipment for municipalities. Smart lighting can be used in many different office and manufacturing settings; the same can be said for air quality monitors.

As the number and type of connected devices used in the enterprise increases, organizations need to be aware of how best to secure these new endpoints. The expanded attack surface of IoT devices makes it harder for security teams to protect critical data, as well as monitor what is and isn't connected to corporate networks. Regardless, something must be done to resolve these challenges.

Cybercriminal Tactics Targeting IoT



Financially motivated cybercriminals and nation-states have distinct goals and tactics when targeting the Internet of Things. Groups seeking to exfiltrate data and sell it might use IoT devices as an initial access point and then move laterally along the network. This would also be the pathway for ransomware attacks that include encryption and then extortion.

In the case of nation-states, the goal may be to use IoT devices as a way to shut down or disrupt key infrastructure services. Nation-state-sponsored groups often use their abilities to complicate operations for their targets, rather than extort money from their targets. Notable exceptions are North Korean groups that conduct ransomware operations to fund the government.

IoT devices are a perfect candidate for botnets. [The Mirai botnet](#) that was used for a distributed denial of service (DDoS) attack against domain services provider Dyn in October 2016 is a good example. Mirai infects smart devices that run on ARC processors and converts them into a network of remotely controlled bots. This botnet is then used to launch DDoS attacks. The attack on Dyn involved 100,000 infected IoT devices in their attack.

Since it first appeared in 2016, the Mirai botnet has spawned several new variants. These other botnets have similar high-level architecture and functionality to Mirai but target other IoT devices or protocols. For example, [Okiru](#) focuses on the Argonaut RISC Core embedded microprocessors that can be found in a variety of IoT devices, while the [Satori](#) variant targets specific versions of the Iteris Vantage Velocity field units commonly used for traffic management operations. PureMasuta weaponizes the HNAP bug in D-Link devices, while the OMG strain transforms IoT devices into proxies for threat actors to remain anonymous.

Threat actors are using IoT devices as part of their attacks. [Nokia found in their 2023 threat intelligence report](#) that the number of IoT devices involved in DDoS attacks has increased five-fold over the past year, with the total number of devices increasing from 200,000 to 1 million, for an estimated global financial loss of \$2.5 billion. Cybercriminals always make use of what works, so it's unsurprising that they're targeting connected devices as part of their attack chains.

They're also tending to use legacy vulnerabilities, likely expecting that their targets either have not or could not resolve those issues. According to [Malwarebytes research](#), 34 of the 39 most-used IoT exploits have existed in these devices for at least three years. In 66% of attacks, threat actors would try to deploy the botnet malware Mirai and Gafgyt. Both of these attacks use older weaknesses on products still in use.

Cybercriminals also have some variety to choose from in IoT. [Zscaler](#) found that there are more than 350 unique malware attack payloads among IoT threats, highlighting the diversity of vulnerabilities that threat actors actively exploit. One interesting point is that nearly [75% of exploited Common Weakness Enumerations \(CVEs\)](#) are command injection vulnerabilities that cybercriminals can use to download and execute stager scripts or malicious binaries. Cybercriminals have taken notice that Internet of Things devices are plentiful and often lack security. They've already exploited this opportunity to gain initial access to their targets. Organizations seeking to protect their critical systems need a new, more holistic approach to their defense strategy as a result.



What Cybercriminals Want

- Steal Confidential and Proprietary Data
- IoT Ransomware Extortion
- Shut Down or Disrupt Services
- Create IoT Botnets
- Data Alteration



The High Cost of Doing Nothing



Enterprises with a large number of IoT devices have to be proactive in their defenses. Doing nothing, or “security through obscurity,” is not a valid practice in this era of increased attack pace. The cost of potential operational downtime and disruption, for example, could be [\\$88.00 per hour lost](#).

This direct impact of recovering from a breach would be bad enough, except there are current and proposed regulatory fines in geographies worldwide. The General Data Protection Regulation (GDPR), for instance, imposes fines of up to €20 million or 4% of global turnover for violations of its provisions. In 2020, for example, Marriott International was fined \$23.8 million by the UK’s Information Commissioner’s Office (ICO) for violating GDPR regulations. The hotel chain was accused of not performing proper due diligence when it acquired Starwood Hotels in 2016, which had experienced a data breach that exposed customer data.

In the United States, [the SEC created new cybersecurity reporting rules](#) for public companies that look like it might ensnare private firms as well. Even before those rules, the SEC has levied fines against companies for data breaches.

- Morgan Stanley paid \$150 million to the SEC in 2021 after a 2019 data breach wherein they were accused of failing to adequately monitor employee access to customer data. The breach resulted from Morgan Stanley allowing an employee to access and copy customer data without authorization.
- Yahoo was fined \$35 million in 2017 resulting from a 2014 data breach wherein the SEC said that the company didn’t inform investors about the breach promptly enough.
- While SolarWinds was not fined by the SEC, the agency nevertheless brought charges against the company that they weren’t forthcoming about cybersecurity practices in the wake of the December 2020 incident that impacted thousands of companies.

Similarly, [violating the Health Insurance Portability and Accountability Act \(HIPAA\)](#) carries a fine that's calculated based on the number of medical records exposed. Fines range from \$50 to \$50,000 per record, with an annual maximum of \$1.5 million per year, but organizations can be assessed the maximum fine for multiple years, and may even face prison time ranging from one year to 10 years.

In the United Kingdom, a breach of the [NIS Cyber Security Directive](#) can lead to fines of up to £17 million. The NIS, which is a European Union law, was implemented in the UK as The Network and Information Systems Regulation 2018, and applies to:

- Operators of essential services (OES) in the UK's energy, transport, health, water, and digital infrastructure sectors; and
- Digital service providers (DSPs) are divided into three groups: online search engines, online marketplaces, and Cloud computing services.

Companies that do business in the UK need to be very closely aware of this fine and what category they fall into. This cybersecurity directive also aligns with a similar regulation in the EU, where different countries can define their own fines to levy for violations.

With these regulations around the world, the risk of facing significant fines globally is substantial, especially if organizations have not fully implemented as many protections as possible. This is in addition to the most

expensive component of a cyberattack – information loss – which represents [43% of the total costs](#) of an attack. Regulatory fines compound that financial impact, so it's beneficial to roll out a defensive strategy that encapsulates every aspect of operations.

Organizations also risk the loss of intellectual property from a successful cyberattack. The loss of IP is among the less visible costs of an attack, including lost contract revenue, potential devaluation of the company's trade name, and damaged or lost customer relationships. A data breach can cost a company an average of \$1.3 million in lost business, [according to IBM research](#), and also lead to an increase in the pricing of business offerings for 57% of companies.

In the case of ransomware attacks specifically, the cost of recovery is nearly \$2 million [in direct financial impact](#). Moreover, there is legal liability in paying any ransom as the [U.S. Office of Foreign Assets Control in the Treasury Department](#) will fine any company that pays the ransom to decrypt its files. According to IoT World Today, in fact, Verizon Business Network Services agreed to pay a \$4 million penalty for failing to maintain cybersecurity standards.

Choosing to pursue a business-as-usual approach to IoT security or not doing anything extra to protect connected devices is not an option. Threat actors will continue to target industries with IoT devices and without, behooving companies of all sizes to improve their connected device security. In the next section, we will enumerate key attacks in several industry sectors to illustrate the security challenges.

Cyber Insurance Is Not Enough



Cyber insurance is designed to cover financial losses from successful cyberattacks. Companies have relied on these policies as key parts of limiting the fallout from recovery operations. Unfortunately, the rise in ransomware attacks globally has led many insurers to limit what they will pay for or cap the amount of the payout.

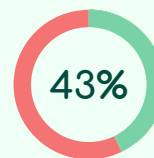
Mondelez International in 2022 settled its lawsuit against Zurich American Insurance Company over claims that the insurer refused to cover the more than \$100 million in costs that Mondelez experienced following a 2017 cyberattack. Mondelez fell victim to the NotPetya ransomware gang in 2017, and Zurich denied their claim in 2018 under a war exclusion clause because of the state-sponsored nature of the NotPetya ransomware.

Multiple cyber insurance companies have followed suit to exclude certain payouts. Lloyd's of London, for example, told companies in its network to exclude payouts for nation-state cyberattacks. The shift toward coverage limits and capped payouts means companies can't necessarily rely on their insurance policies to recoup financial losses. The January 2024 settlement in the case of Merck versus its cyber insurer further complicates the issue. The insurer eventually settled to avoid a court decision demanding they cover nation-state attacks. It's still unclear now if the language of war will weaken cyber insurance payouts.

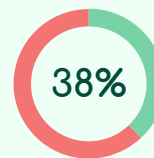
More importantly, however, cybersecurity insurance doesn't cover reputational damage. [According to Varonis](#), 80% of consumers will defect from a business if they don't think their data is secure. There's no guarantee even with cyber insurance the claims will pay out. Recoveries take significant time, effort, expertise, and expense to process for staff that is trying to remediate security issues. Business interruption claims, probably the most germane claim type to this situation rely heavily on assumptions; as a result, they take longer to adjudicate.

Also, most cyber insurance policies have stringent requirements in place for layered defense systems. If those systems are not operational or it's deemed anything was missing during the incident, the policy is considered invalid. It's not an umbrella protection and is in fact written to protect the insurance company. According to one report, the following are the top five reasons cyber insurers denied coverage.

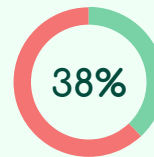
Top Five Reasons Cyber Insurers Denied Coverage



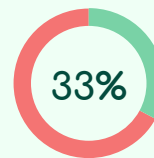
Lack of Security Protocols in Place



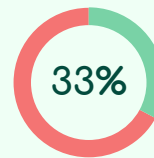
Internal Bad Actor



Human Errors like Misconfigurations, Lost Devices



Acts of War



Did not Follow Cybersecurity Compliance Procedures

Understanding the typical coverage provisions and exclusions is critical when trying to untangle this web of coverage issues. Whether your cyber insurance policy pays out or not can depend on how compliant your security is with standard cybersecurity frameworks. Also, your proof of active security controls may influence this payout. Compliance frameworks are used to ensure that your company meets minimum standards of prevention, and might include:

Mandatory Regulations:

- GDPR
- HIPAA
- NIS2 Directive
- SEC

Voluntary Frameworks:

- CIS Controls Framework
- CISA Cybersecurity Framework
- COBIT Framework
- HITRUST Cybersecurity Framework (CSF)
- ISO 27001
- European Union Agency for Cybersecurity (ENISA) National Capabilities Assessment Framework
- NIST Cybersecurity Framework
- PCI DSS [mandatory to hold credit card information]
- SOC 2 Compliance

Industry Guidelines and Standards:

- DNV NIAHO
- FDA Post-Market Guidance for Cybersecurity
- HHS 405(d)
- IEC/ISO 80001
- NERC CIP
- The Joint Commission (TJC)

Cyber insurance recoveries take significant time, effort, expertise, and expense. These sorts of business interruption claims rely heavily on assumptions and take some time to adjudicate. Although cyber insurance remains a key facet of a defensive strategy, the challenges inherent in ensuring any sort of recovery from premiums paid means that such policies can't be relied upon.

Even with cyber insurance coverage, organizations can remain on the hook for millions of dollars in damages related to recovery. Because insurance policies are capped on their payouts, a successful incident may still cost a substantial sum. Moreover, insurance premiums will soar following any claims against the policy. In 2022 alone, cyber insurance premiums surged 50%; reaching \$7.2 billion in premiums collected from [policies written by insurers](#). Cybercriminals have specific tactics to target IoT devices at enterprises. These tactics and others make it clear that cyber insurance can only be part of the solution.

The infographic features a central title 'THE IMPACT OF A Cyberattack' in a large, dark green font. Above the title is a shield icon with a keyhole. Below the title are five horizontal bars, each with a circular icon on the left and a text label on the right. The icons are: a camera for 'Operational Downtime', a gavel for 'Regulatory Fines', a globe with a padlock for 'Loss of IP', a ribbon award for 'Regulatory Damage', and a bar chart with a downward arrow and a dollar sign for 'Loss of Revenue'. The background is light green with faint network diagrams.

IoT Security Predictions for 2024



The number of IoT devices deployed exploded in 2023. There are 15.14 billion connected devices that were brought online in the past 12 months, [with another 2 billion expected to come online in 2024](#). The sheer volume of IoT devices connecting to the internet at any given time complicates every security practitioner's job.

Over the next 12 months, we expect IoT security teams to prioritize these areas:

1 The human element of their security programs

According to [Gartner's recent research](#), 50% of CISOs are going to formally adopt human-centric design practices into their cybersecurity programs to minimize operational friction and maximize control adoption. Ideally, this will minimize the friction in keeping enterprises secure and allow employees to get more work done.

2 Staffing shortages in cybersecurity teams

[ISC² recently found that there](#) remains a shortage of 4 million cybersecurity professionals, despite a 10% growth in the cybersecurity workforce over the preceding 12 months. This shortage of skilled professionals is going to become an even bigger security risk in 2024. People with both cybersecurity and IoT knowledge are rare. The lack of skills at most organizations means that new devices aren't getting the attention needed to be protected. If the staffing shortage isn't ameliorated, more attacks could occur through inexpertly defended IoT devices.

3 Shadow IoT will become more common

As IoT becomes more common in the enterprise, there will be a growth in the amount of shadow IoT. Gartner's research showed that by 2027, [75% of employees](#) will acquire, modify, or create technology that IT lacks insight into – up from 41% in 2022. This is problematic in general, especially given the risks inherent in a lack of insight into the full attack surface. The increase in shadow IoT is going to create a bigger risk of a cyberattack for many organizations. Security teams would do well to deploy technologies that capture the full scope of devices connected to their infrastructure.

4 Artificial intelligence will be a bigger issue

The rise of tools like GitHub Copilot and other AI-generated code means that there is a bigger risk of security issues being inserted into IoT devices from a firmware perspective. There are already major issues with IoT devices in terms of secure coding practices not being standard throughout the industry. As AI tools become more broadly used and integrated into more CI/CD pipelines, security professionals will need to be aware of any potential vulnerabilities hard-coded into IoT devices that are already difficult to patch.

5 Vulnerabilities in IoT Devices

Internet of Things devices are incredibly difficult to patch at the best of times. In 2024, the ascendance of IoT systems in more organizations will put vulnerabilities in things like [security cameras](#), pacemakers, printers, and other connected devices more in focus. Security teams at organizations of all sizes should take a hard look at the IoT systems included in their corporate networks for a more cohesive approach to patching or mitigating vulnerabilities.

6 More need for threat detection, investigation, and response capabilities

As more IoT devices come online, organizations will need to seek out systems that can detect anomalous behavior and centralize the investigation of IoT-based attacks. IoT devices also cause substantive growth in organizational attack surfaces, necessitating the use of exposure management capabilities to see precisely what traffic is flowing to and from IoT systems within the corporate network. As a result, the ability to monitor for threats, investigate alerts, and respond to active incidents will become even more crucial.

These changes over the next year could provide additional risk or resolve some of the lingering challenges with IoT. Regardless of whether these occur or not, however, the reality is that IoT devices will continue to proliferate and create new risks to account for.

Questions to Assess IoT Security Risk

In the year ahead, security teams need to adapt to the changing nature of protecting the IoT. This will include considering the human element of their program, scaling within their means to account for staffing challenges, and understanding the spread of shadow IoT. This is alongside the risks of artificial intelligence, a vulnerable IoT device architecture, and a greater need for robust threat detection.

Who is responsible for IoT device inventory?

How are IoT vulnerabilities detected?

How are vulnerability remediations prioritized?

What risk level is acceptable?

What potential risks from third parties exist?

Are high-risk devices identifiable?

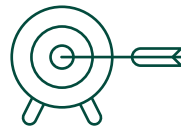
How are in-process attacks detected?

Are there snapshots of ideal-state configurations to aid disaster recovery?

Is Incident response aided by data packet capture?

Is there a one-size-fits-all approach to segregating vulnerable devices?

The Most Targeted Industries in 2023



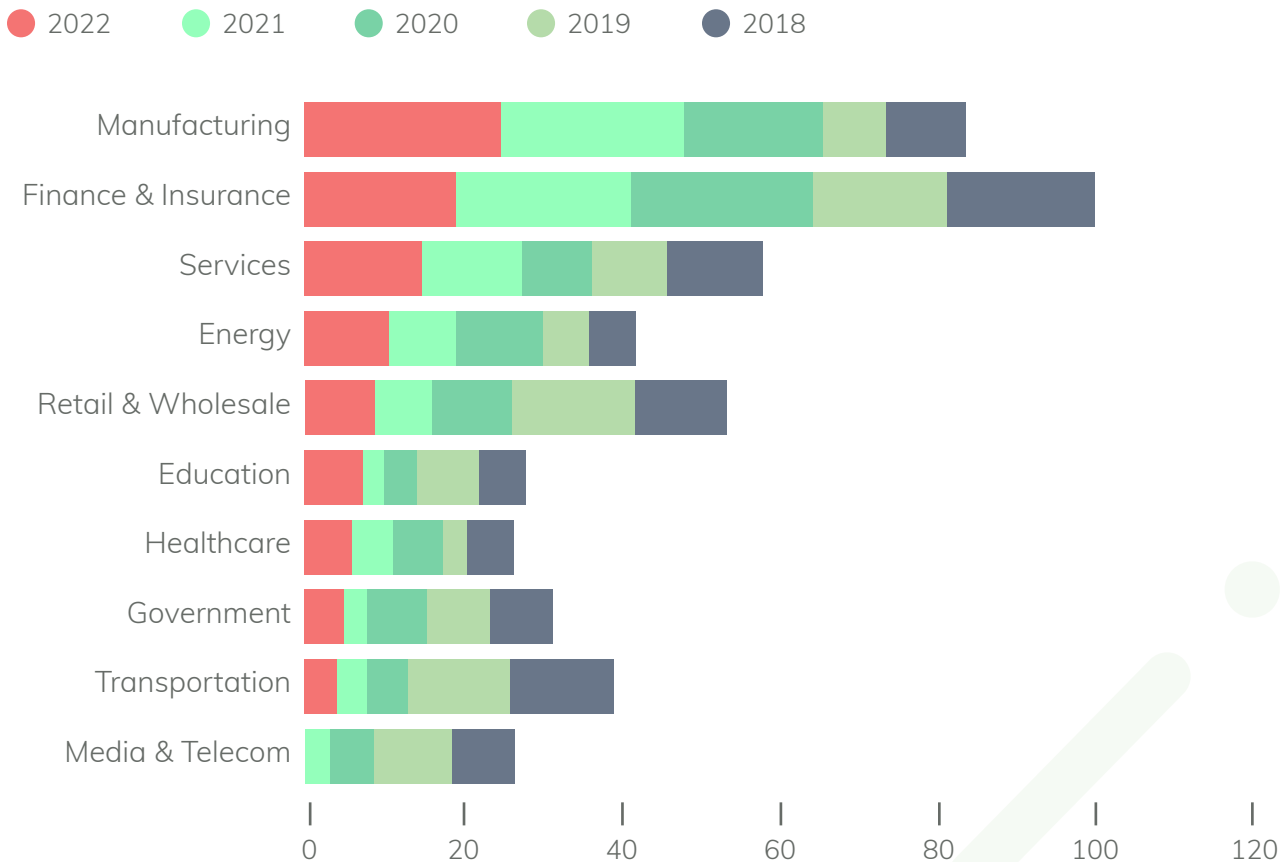
Within the past year, a few industries have borne the brunt of the increased number of cyberattacks. [According to IBM X-Force data](#), this has included manufacturing, services firms, and energy companies among others. Manufacturing companies sitting near the top of the list of attacked firms shouldn't be surprising. Firms across the various forms of manufacturing have a lot of intellectual property and proprietary designs; financially motivated cybercriminals can sell those designs to foreign governments or foreign corporations where intellectual property laws are less stringent.

Inclusive of this data from IBM, there are a few industries that we're going to examine in terms of recent attacks. This will include specific examples, as well as an examination of the reasons why threat actors view these spaces as potentially valuable targets.

It's important to note that these attacks, while not necessarily originating with IoT devices, are nevertheless incredibly damaging to operations. An attack can start anywhere in critical systems, and the increased number of IoT endpoints means that they can be used for lateral movement deeper into the organization as well as an origin point. Let's now examine some key attacks in different sectors, starting with manufacturing.

At the Top of an Unfortunate List

Hackers have increasingly targeted manufacturing firms and de-emphasized media and transportation companies



Source: [IBM X-Force incident response data](#)

Recent Attacks on Manufacturing and the Consequences



Manufacturing companies experienced 54.5% of attacks in 2023, according to Zscaler research, with an average of 6,000 attacks against them per week. Given that manufacturing companies tend to have tens and hundreds of thousands of OT and IoT devices in their networks, they have some unique weaknesses among other firms.

Manufacturing companies are also some of the most critical to a country's economy. Interrupting operations of the right manufacturing company can cause failures throughout certain market sectors.

A few of the most recent attacks on manufactures include:

- ✚ Ingersoll Rand, a maker of compressors, experienced a ransomware attack in March 2023 where malicious actors leaked an estimated 3% of stolen data.
- ✚ Johnson Controls International experienced a ransomware attack that also impacted two of its subsidiaries and encrypted the company's VMware ESXi machines. Malicious actors stole more than 27 terabytes of data in the attack, potentially also including Department of Homeland Security floor plans and security information.
- ✚ Fortive Corp, which makes test and measurement tools and asset management software, reported a [\\$5 million one-time expense](#) on its earnings report related to the remediation and operational impact of a ransomware attack from BlackBasta.
- ✚ Mueller Water Products, Inc. reported a cyberattack in October 2023 that affected its IT and OT systems alike, and wasn't fully contained until the end of November. Mueller is one of the largest manufacturers and distributors of fire hydrants, gate valves, and other water infrastructure products in North America. They delayed filing a 10-K with the SEC and didn't resume normal operations until mid-December.



Manufacturers can expect to see far more threats in the coming years given the complexity of protecting OT and the rise of industrial IoT systems that are more connected to the internet now. Organizations in this space need to take a hard look at how they're defending critical systems. This is also true for healthcare companies, who need to be especially aware for protecting patient safety.

Recent Attacks on Healthcare and the Consequences



A few of the most recent attacks on hospitals include:

- 🎯 McLaren Health Care in November 2023 said that a data breach between late July and August affected 2.2 million people. McLaren is a Michigan-based chain of 14 hospitals with revenues of \$6.6 billion across the entire system. Through its network, it extends into Indiana as well. The company announced that threat actors had exfiltrated personal data including Social Security numbers, health insurance information, and other personal health data.
- 🎯 Sutter Health revealed that more than 845,000 customers had their personal data exposed following a breach of its third-party messaging service because of the MOVEit file transfer hack in May. Attackers may have accessed patient's names, birthdates, provider names, health insurance data, treatment cost details, diagnosis, and treatment information but not any financial information or Social Security numbers.
- 🎯 HCA Healthcare disclosed a data breach in July 2023 that may have affected up to 11 million people in what could be the largest breach of the year. The theft was from external storage used for formatting email messages, according to the company, and didn't include any personal financial or health information. What it did include was patient names, addresses, dates of birth, and information on patient service dates, locations, and the dates for the next appointments.

Healthcare's unique requirements for patient safety and the threat to life from service disruptions continue to keep this industry in cybercriminals' crosshairs. Healthcare companies tend to spend on average 6% of their IT budget on security. This doesn't leave a lot for securing critical systems. When paired with their low tolerance for downtime, healthcare companies and hospitals in particular are very attractive for ransomware groups. In fact, [25% of Americans](#) were impacted by healthcare data breaches in 2023.

Healthcare systems that have started to use more IoT devices, including nuclear medicine equipment, connected pacemakers, or other Internet of Medical Things (IoMT) devices open themselves up to additional risk. Although the attacks outlined below may not originate with network-accessible and feature-limited devices, the reality is that adding new technology to a healthcare network adds risk.

Healthcare companies will likely continue being attractive targets for threat actors. The personal health information that hospitals and other healthcare organizations store is one of the few pieces of data that can't be changed following a breach. Credit card numbers are only good until financial services firms change them; Social Security numbers cannot be changed and can be readily used for identity theft.

Healthcare organizations would do well to shift some additional spend to cybersecurity, especially in light of the risk of HIPAA fines and a greater focus on data privacy in the year ahead.

Recent Attacks Gaming and Casinos and the Consequences



Video games and casino gaming have experienced their own slate of cyberattacks. Attacks against the video game industry and gamers spiked during the pandemic lockdown year of 2020, with more than 240 million web attacks that year alone. This was a 340% growth over the previous year, made easier with a shift to cloud gaming. Attacks against the video game industry could occur for a few reasons, including wanting to leak new games or wanting to find ways to steal from other players on massive online games.

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.

Here are a few of the more recent attacks or suspected breaches in the casino and gaming industry:



🎯 Caesars Entertainment confirmed a September 2023 theft of its loyalty program database. The casino chain paid a ransom of around \$15 million to avoid the publication of the stolen data. The ransomware gang had originally asked for \$30 million. The chain filed an 8-K with the SEC to report the attack in accordance with new rules.

🎯 Ubisoft, the video game giant, is investigating a possible cyberattack revealed at the end of December 2023. There's no confirmation that a data breach has occurred, but security researchers contacted the company with the possibility that someone tried to steal Rainbow Six Siege user data.

🎯 MGM Resorts, only a few days after the Caesars hack, also experienced a ransomware attack. They did not pay any ransom, opting instead to shut down a substantial portion of their systems to contain the damage. They expected the attack to result in a financial loss of \$100 million in their third-quarter earnings.

As casinos continue their digital transformation and video game companies shift to deploying their games in the cloud, the risks of data breaches and ransomware attacks will continue to rise. These gaming companies need to be aware of this and shift their security strategies accordingly.

Recent Attacks on Higher Education and the Consequences



A few of the most recent attacks on universities include:

- 🎯 The University of Michigan suffered a data breach in August 2023 that compromised data from 230,000 students, alumni, and employees. The university disconnected its campus network and launched an investigation into the source of the breach.
- 🎯 The Stanford University Department of Public Safety was attacked in October 2023, with the Akira ransomware gang claiming they stole 430 GB of campus police data. The university confirmed the attack in November.
- 🎯 Mount Saint Mary College in Newburgh, New York, confirmed a December 2022 ransomware attack following the group Vice Society claiming credit on its leak site. The college said in their statement that they detected and stopped the attack, months after keeping the incident silent.
- 🎯 The University of Missouri System was caught up in the MOVEit file transfer breach through one of its third-party vendors used in enrollment operations. The university system said that some of its data had been compromised but did not clarify because of the ongoing investigation.



The education sector in general has experienced a substantial increase in malware attacks. Since 2023, the number of attacks against the sector has increased by 961%, according to [Zscaler data](#). Education is another industry that tends to have limited investment in cybersecurity. The bulk of IT spend in education relates to increasing access for students and teachers.

Education tends to have the same low tolerance for downtime as healthcare. So it makes sense that education would be an attractive target for threat actors. When these attacks are conducted, the limited cybersecurity investment means that downtime is severe. Between 2022 and 2023, in fact, the average amount of downtime for educational institutions caused by ransomware disruptions has increased from 7.9 days to 11.6 days.

Higher education will continue to be a target for ransomware gangs in the future. Their broad use of third parties and extensive IoT devices from students and teachers make them vulnerable.




Recent Attacks on Transportation and Logistics and the Consequences



The transportation and logistics sector includes a variety of sub-industries, including airlines, passenger and freight trains, trucking companies, third-party logistics vendors, and container shipping vendors. Attacks against this sector can be especially damaging. In 2017, NotPetya brought container shipping vendor Maersk's operations to a halt. This had no small impact on global trade at the time. Maersk is the single largest global oceangoing shipping company, with responsibility for 76 ports globally, 800 shipping vessels, and one-fifth of global trade..

Companies in this sector like Maersk are so integrated and so essential that they have many relationships with companies around the world. They also often have antiquated systems as a result of these relationships; there's no guarantee that every country will have the same level of infrastructure. In the Maersk breach, Ghana's unreliable infrastructure is simultaneously what saved the day and also what made it difficult to restore the global system from a lone surviving uncorrupted data image.

Recent attacks on transportation companies include:

-  In June, the personal information of around 8,000 pilots, who applied to jobs at American Airlines and Southwest Airlines was stolen from Pilot Credentials, a recruiting company used by the airlines. Both airlines moved applicant information to internal systems following the attack.
-  KNP Logistics blamed a ransomware attack for the company entering administration, with 730 employees losing their jobs. The UK haulage firm was one of the largest independent operators in the country, but unfortunately, the ransomware attack caused them to struggle to find additional investment and funding.
-  Expeditors International of Washington, Inc., shut down most of its operating and accounting systems in February 2022 in the wake of a successful cyberattack. Although they sought to protect data and infrastructure, they unfortunately limited their ability to ship freight, manage customs processing, and distribute customers' products. The outage went on for three weeks and led to a class action lawsuit from customers including iRobot and others.



Transportation and logistics companies are integral to the fabric of modern society. Firms like KNP Logistics and Expeditors International ship freight from factories to stores and necessary materials to manufacturers. If they're not able to operate, then other companies can't function. That's the core of the lawsuit against Expeditors and the proof of how damaging an attack against transportation companies can be. Few would feel this more prominently than life sciences companies transporting critical medication, who are also under threat.

Recent Attacks on Life Sciences and the Consequences



Life Sciences companies including those in pharmaceuticals, biologics, biotech, medical devices, food processing, and others have increased their use of sensitive customer data in the past few years. As a result of this, plus valuable intellectual property and high turnovers, the average [cost of a data breach](#) in pharmaceuticals was \$4.82 million in 2023.

Life Sciences companies are heavily targeted in general. The CISO of global pharmaceutical company Johnson & Johnson, for example, said in 2021 that the company experienced 15.5 billion potential cyberattacks per day. There's no telling how that may have increased in the past few years.

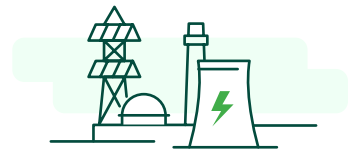
Here are some recent attacks on Life Sciences companies:

🎯 [Novartis in June 2022](#) saw its data hijacked by Industrial Spy, a well-known online extortion ring. The group claimed they stole data related to DNA and RNA-based technologies from the Swiss pharmaceutical company.

- 🎯 PharMerica, one of the largest providers of pharmacy services in the United States, revealed in March that an unknown actor accessed its systems in March and extracted personal data pertaining to 5.8 million individuals. PharMerica operates 2,500 facilities directly and over 3,100 pharmacy and healthcare programs throughout the country. They notified affected individuals and the next-of-kin for any deceased people whose personal information was impacted.
- 🎯 Pharmaceutical giant Merck lost \$1.4 billion in 2017's NotPetya attack linked to Russian threat actors. The attack started with an infection in Ukrainian accounting software, eventually spreading to 65 countries. Merck was one of the biggest victims and has been locked in a lengthy court fight against insurers trying to avoid paying out. [Just recently, the courts ruled that insurers couldn't use the war exclusion clause](#) to avoid making a payout in this case.
- 🎯 Postmeds, a mail-order pharmacy, revealed in late August that the personal data of more than 2.3 million patients was exposed in a cyberattack.
- 🎯 Enzo Biochem in April 2023 filed an 8-K with the SEC that the test information and personal data of nearly 2.5 million people were compromised in a ransomware attack. The company is still investigating the incident but noted that may continue to incur remediation-related expenses above what it has already paid.

Life Sciences companies would do well to account for their critical equipment and protect it against threats. Cybercriminals and nation-state groups seeking to either steal data or intellectual property will continue to target them. This state will require tighter analysis of security risks and a more nuanced method of protecting connected devices and other necessary manufacturing or scientific equipment. And that's even outside of discussing the threats facing critical infrastructure.

Recent Attacks on Utilities and Critical Infrastructure and the Consequences



Critical infrastructure companies including oil and gas facilities, water treatment plants, electric companies, and sewer facilities are under threat mainly from nation-state groups seeking to disrupt their government's enemies. Disrupt operations at an electricity company or a water treatment plant, and it's possible to sow chaos in a society.

In terms of IoT, many critical infrastructure companies have remote monitoring tools implemented through their infrastructure. An oil and gas pipeline typically runs through miles of wilderness and has sensors all along its length to track the liquid crude as it travels from extractors to refiners. Water treatment plants might have sensors spread throughout their operations, and electric companies could have internet-enabled transformers tracking power flow through their systems.

It's not just cyberattacks. Utilities and other critical infrastructure reported 60 incidents in the first three months of 2023 that they characterized as physical threats or attacks on major electric grid infrastructure, in addition to two cyberattacks, [according to mandatory disclosures with the Department of Energy](#). This is more than double the same period in 2022 and is indicative of the desire of criminals to cause mass blackouts in the United States. Electric companies are especially vulnerable to physical attacks with the need to have remote substations to move power through their regions.

Different critical infrastructure categories experience distinct threats. In terms of water companies, an IoT breach won't necessarily stop operational technology from functioning or creating downtime.

There are also rural municipal water companies that experience a higher number of threats because of their limited budgets. Two recent examples are:

⊕ The Municipal Water Authority of Aliquippa in Pittsburgh had to shut down its OT systems after a cyberattack from the Iran-backed group "Cyber Av3ngers" on one of its booster stations. The attack shut down equipment that monitors water pressure at the station, forcing the water company to switch to manual monitoring.



⊕ [At least 10 more water facilities](#) throughout the United States were hacked through the same method the Cyber Av3ngers used to breach the Aliquippa water company, according to federal investigators. The devices that the Iranian group shut down were manufactured in Israel and displayed a message that said all Israeli tech is fair game for the Cyber Av3ngers.

⊕ The Municipal Water Division of Oldsmar, Florida, had to defend against a poisoning attack. Someone hacked into a utility control network and raised levels of sodium hydroxide to over 100 times their normal concentrations. Sodium hydroxide is dangerous in large quantities but is safely used in everyday water treatment. An operator who noticed the hack in real time - by seeing his mouse cursor move by itself - stopped the chemicals from reaching the water supply.

With power companies, the same trends apply. Co-ops and rural companies are getting targeted because they're the ones with the smallest amount of resources. In 2022, there were a total of [1,665 security incidents](#) involving the U.S. and Canadian power grids; 60 of those incidents led to outages. Although IoT attacks may not cause major disruptions given how they're connected to a network, the reality is that they can still impact energy company terminals and other IT rather than OT. For Example:

🎯 In 2021, Colorado cooperative Delta-Montrose Electric Association (DMEA) was hit by a "malicious" cyberattack and left without payment processing, billing, and other internal systems. It took over a month for those systems to come back online. The utility said it suffered a significant data loss, but the distribution grid was not impacted and there was "no breach of sensitive data within our network environment".

🎯 [Nearly two dozen Danish energy companies](#) were attacked in May 2023 in three successive waves of attacks. This was the largest cyberattack in Danish history and resulted in several of the power companies shutting off their internet connections to protect critical systems.

🎯 It's not only power companies directly that are impacted. Chicago-based engineering firm Sargent & Lundy experienced a ransomware attack in October 2022. Sargent & Lundy has designed more than 900 power stations and has thousands of miles of power systems that hold sensitive data. Data on electrical systems was exfiltrated in the attack, and at the time there was no indication of any downstream impacts. But that doesn't mean power companies can relax either.

Oil and gas companies typically have larger organizations with distributed networks and riskier IoT assets because of how geographically dispersed their operations are. Overall, these companies are less regulated in terms of how and where to invest in cybersecurity. Everything relies on IT defenses as opposed to the OT side of things with other utility and critical infrastructure companies.

That said, successful cyberattacks in the oil and gas industry can have massive societal impacts. There could be consumer-level gas shortages, triggering hoarding behavior at the pump and leading to broader chaos. In some cases, that may be the goal of the cyberattack in the first place.

🎯 In May 2021, financially motivated cybercriminals launched a ransomware attack on Colonial Pipeline. The hack locked up IoT sensors on the pipeline, making it impossible for the company to track how much to bill customers. In response, the company shut down all 5,500 miles of pipeline. This pipeline makes up 45% of the East Coast's supply of diesel, petrol, and jet fuel. Because of the shutdown, there were fuel shortages and panic buying in multiple U.S. states.

🎯 Suncor Energy, a Canadian oil and gas company, experienced a cyberattack in June that one expert said would likely cost the company millions of dollars in recovery. Customers trying to get gas at Suncor Petro-Canada retail locations were unable to pay with credit or debit cards while the company recovered. [It took until nearly August](#) to almost completely recover regular operations.

🎯 ExxonMobil was disrupted in December 2019 by a Ryuk ransomware attack. Ryuk specifically impacted the company's downstream business, which includes refining, chemical production, and distribution of petroleum products. Operations of the company were substantially impacted and took some time to recover.

🎯 In 2017, cyberattackers using a new Triton malware attacked the safety systems at Saudi Aramco, the world's largest oil company. This was the first example of malware used to directly target the safety systems of a critical infrastructure facility. Aramco initially denied the attack. It didn't come to light until a report was published in Foreign Policy magazine detailing the attack's progression.

These cyberattacks across multiple industries are indicative of how quickly things can change. Although they may not have originated in IoT devices, the reality is that connected equipment can easily be used to exacerbate attacks if proper defenses are not put in place. Companies would do well to evaluate their security approaches, including how they integrate things like cyber insurance into their protection plans.

A Holistic Approach to IoT Security



A holistic, risk-based approach is required to defend your IoT devices. What this means in practice is that the traditional perimeter-centric method of protecting IT assets doesn't scale properly to secure IoT equipment. This is especially true given how quickly IoT devices are deployed and the sheer amount of new assets added to the average attack surface as a result. The key goal here is preventing attacks from spreading; ultimately, this makes an attack less costly because operations are unlikely to be affected.

From a decision-making perspective, this holistic strategy should apply a risk treatment framework of avoid, mitigate, transfer, or accept.

- 01 Avoid or resolve the risk completely, i.e., eliminate or forgo the risk
- 02 Mitigate the risk to reduce the likelihood or impact
- 03 Transfer the risk by moving or assigning it to a third party like cyber insurance
- 04 Accept the risk by choosing not to resolve, transfer, or mitigate

These categories of risk treatment and tolerance should form a decision-making strategy as companies look to reduce their overall cyberattack risk. Risk mitigation should begin with understanding the current state of network infrastructure. Expanding attack surfaces often means that security teams have limited visibility into what's installed on their networks. This is especially true with IoT devices that are often deployed without IT involvement. What's important to understand here is that you can't secure what you don't know about. Aiming for complete visibility is the goal.

Complete visibility in this context of course means far more than having an accurate inventory of your systems. You need to detect any IoT devices attached to your network, as well as create a device profile and classification down to the specific model, operating system, and software version. This is what the Asimily platform does. It defines where devices are on the network and what departments they're in, while also tracking them if and when they move through your locations.

Mitigations come in the form of vulnerability removal (patching) or compensating controls. Often, compensating controls can be quick, require no team coordination, don't have a hidden complexity cost, and remove the same risk as the traditional approach: network segmentation.

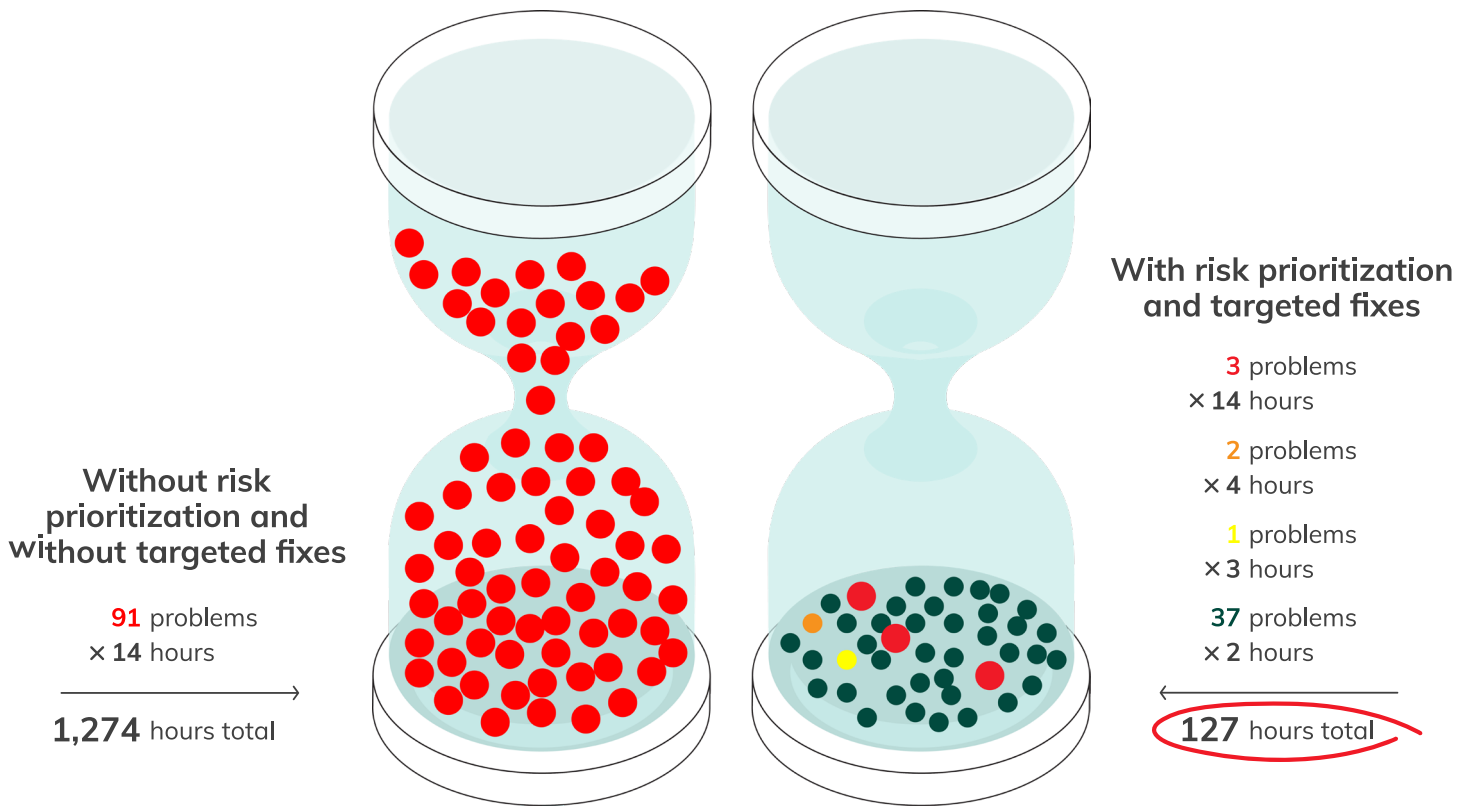
These very targeted fixes, like turning off Remote Desktop Protocol (RDP) access, can protect devices effectively, but only if the hard work of analyzing each vulnerability in context has been done with a risk lens, not a vulnerability lens. Ongoing efforts to apply the least-access principle to all devices are important too.

By using the [MITRE ATT&CK Framework](#) to investigate not only the vulnerability but the kill chain and network context, better risk-based mitigations can be selected. With a preference for simpler fixes, vulnerabilities can be demonstrably nullified, and the risk removed, using low-effort techniques when all else is equal.

Asimily has a database of over 180 targeted fixes (and growing). Each fix, including the RDP example above, is selected and doesn't interfere with the device's operations, removes the vulnerability's risk and is as simple to apply as possible compared to other potential fixes.



How Asimily's Patented Remediation Compares to the Traditional Approach



The opposite of the one-size-fits-all approach to handling vulnerabilities is targeted remediation. An attack is successful when a set of conditions are met, and a series of steps are followed that use a vulnerability. Instead of blocking off the entire system from attackers, which can often be achieved through network segmentation, smaller efforts can be expended to prevent a successful attack.

By changing a pre-condition or halting a step, a potential attack can still be diverted. The fix can still remove the risk, without always addressing the vulnerability head-on with a patch, which may or may not be available or possible for other reasons.

This approach offers several advantages over segmentation and microsegmentation, which are acceptable as last resorts. Targeted remediation usually takes less time and team coordination to remove the same risk. For example, to take a device from a flat network to a micro-segmented network means coordinating with everyone who touches that device or uses its data - upstream or downstream. They may have needs that are not known to the network team responsible for the segmentation effort. Further, there's no complexity tax to the network, which makes it harder to manage going forward.



Develop Baseline Risk KPIs

Holistic risk management benefits from KPIs to measure. As part of crafting your cohesive and holistic approach, these KPIs need to be agreed upon and measured throughout the security and IT organization. A few of the most common ones that Asimily suggests are:

1 Org Risk Score (ORS)

An Org Risk Score is a simple measurement to understand the overall security situation of your company. Asimily rates organizations with a 1 to 100 score, with the higher numbers equalling more risk. Within the Asimily platform, this score is also scaled to the size of the organization, so smaller organizations aren't unduly penalized. The ORS can also take into account IoT and IoMT devices.

2 Mean Time to Resolution

Mean Time to Resolution/Remediation showcases how long it takes to remediate security issues within your systems. A low MTTR is the "gold standard" here, but teams with limited resources might take more time to remediate issues because of their resource constraints. This measure could also change based on the type of issue being remediated at any given time.

3 Quantity of CVEs

This is the raw number of CVEs within your systems. You want the number of identified CVEs in your systems to be kept low or at the very least, within a strict risk tolerance. If there are too many active CVEs in your network, it could be indicative of severe breach risk.

4 Distribution and Severity of Vulnerabilities

This metric helps you understand where the vulnerabilities are and how severe they are. Severity can be a difficult metric to judge. Even though CVEs include a CVSS score to show their relative severity, there might be CVEs with a lower overall risk score that are more impactful in your systems. It all depends on your unique setup and what is required for the CVE to be used.



5 CVEs Remediated

This is the overall number of CVEs remediated in your systems. Theoretically, more remediated or patched CVEs mean that you're more secure. This may not be the case though because of the risk of unknown vulnerabilities, but understanding the number of CVEs remediated per quarter or year at least proves that there's progress on closing security holes.

6 Cost of Risk = (Threat x Vulnerability) x Impact

Understanding the real financial cost of risk is an important KPI to track over time. The calculation for the cost of a risk integrates the likelihood of the threat, combined with the vulnerability score, and measured against the potential impact. If there's a vulnerability in a security camera, for example, that potential impact could be substantial. A weakness in a segmented wireless speaker in your factory, by contrast, may not be that impactful.



Managing and Mitigating IoT Vulnerabilities Effectively

Traditional vulnerability management has involved focusing on patching every single CVE throughout the organization. The idea is that as more weaknesses are patched, you become more secure. While true in theory, the reality is that more than 29,000 vulnerabilities were identified in 2023. There is no feasible way for any security team, no matter how skilled or how large, to patch every single CVE in their architecture.

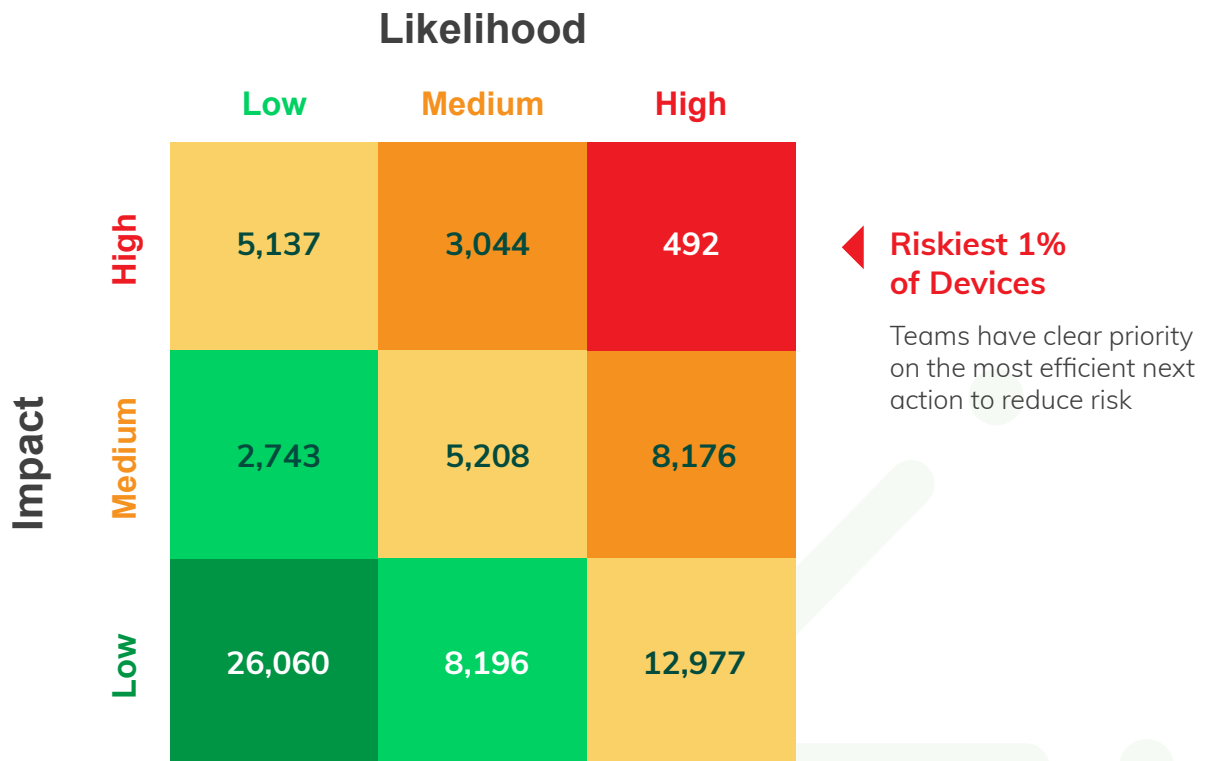
Organizations should do the following instead:

1 Focus limited staff time on the most critical vulnerabilities in their installed context. Public data on severity doesn't take into account the specific setup of each organization's technology infrastructure. The same vulnerability in two different devices configured differently and in different networks can have wildly varying risk levels. Not every one of the 29,000 CVEs is created equal.

2 Deprioritize segmented networks. With a segmented network, teams could de-prioritize certain vulnerabilities. Maybe a particular workstation isn't connected to the network, or maybe it's only tied into a very small cluster. If the risk of a breach is low, vulnerabilities in that system can be a lower priority.

3 Track behaviors and traffic flows via policy management for devices where device or network controls cannot be applied. Some devices can't have the same controls deployed because of exceptions. Tracking behavior flows here can help cybersecurity teams be more efficient.

Another way of prioritizing vulnerabilities is to run risk simulations on your devices. Doing these simulations allows you to more concretely see what would happen if a threat actor gained access to a particular device or network segment. This sort of automated penetration testing or simulation can allow you to make better decisions and also visualize what the potential outcome of changes could be before you make them.



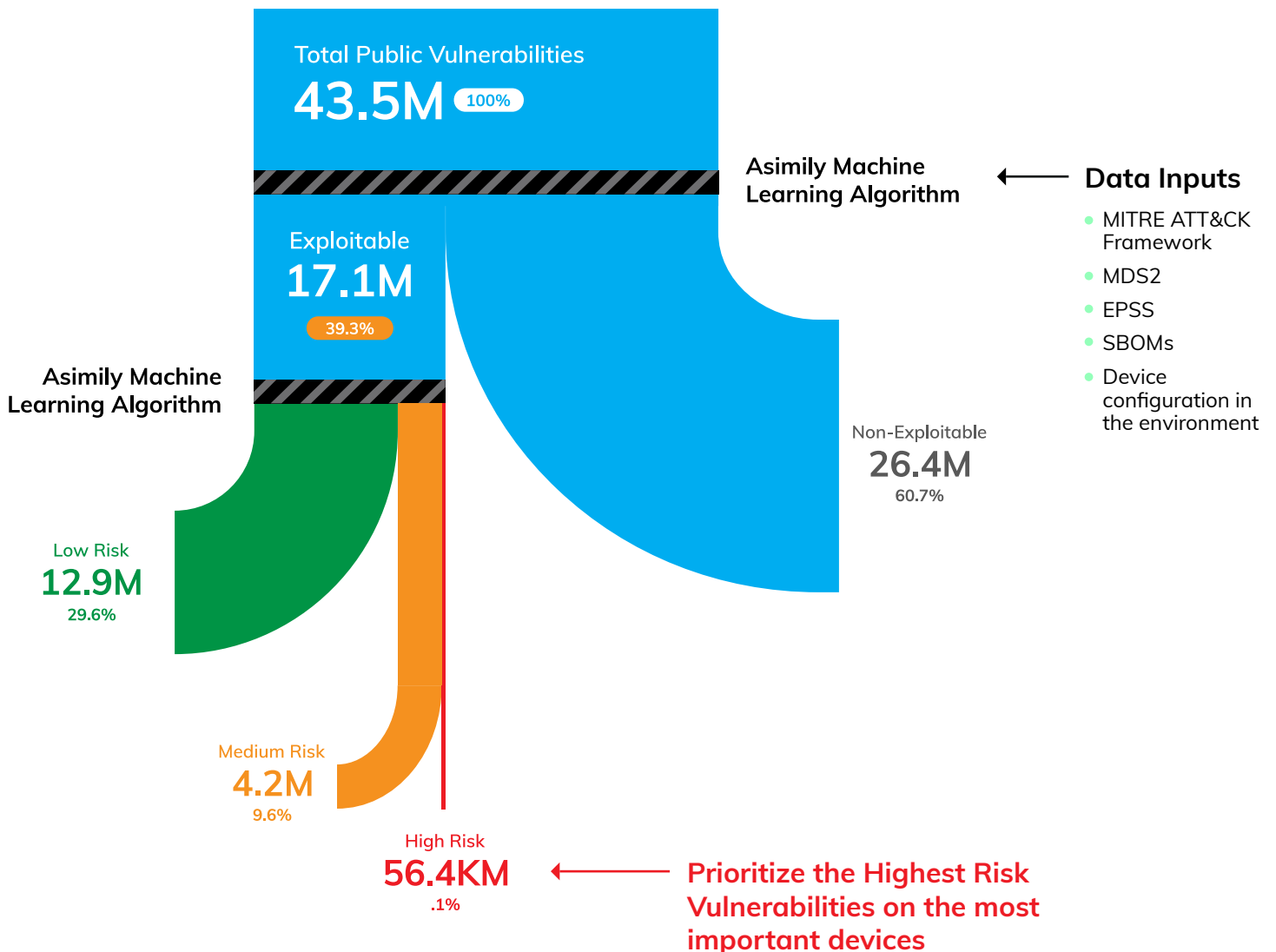
In the case of security alerts, it's vital to understand that around 45% of all alerts are false positives. SOC analysts receive thousands of such alerts per day, and prioritizing alerts on only the most vital or most valuable equipment can help reduce the chance of alert fatigue impacting the ability of security teams to do their jobs effectively.

Asimily prioritizes vulnerabilities that are exploitable in your unique environment in real-time (not just those with publicly available exploits) through our deep contextual recommendation engine. Our proprietary, patented AI engine cross-references vast amounts of data across [MDS2s](#), [SBOMs](#), [EPSS](#), CVEs, the [MITRE ATT&CK framework](#), and [NIST guidelines](#).

Asimily research on device configurations, impacts, and other parameters for real-time recommendations designed for the most efficient use of analyst hours.

Asimily's Vulnerability Mitigation allows customers to be 10x more efficient as our engine is able to narrow theoretical vulnerability information down to about 1% of the original list. This comes from a focus on High-Risk devices, which Asimily classifies as having vulnerabilities with a high likelihood of exploitation on devices with high impact if compromised. Asimily's clinically validated recommendations can easily be applied in a number of ways on the network or device itself.

Patented Exploitability Analysis





Incident Response & Forensic Analysis

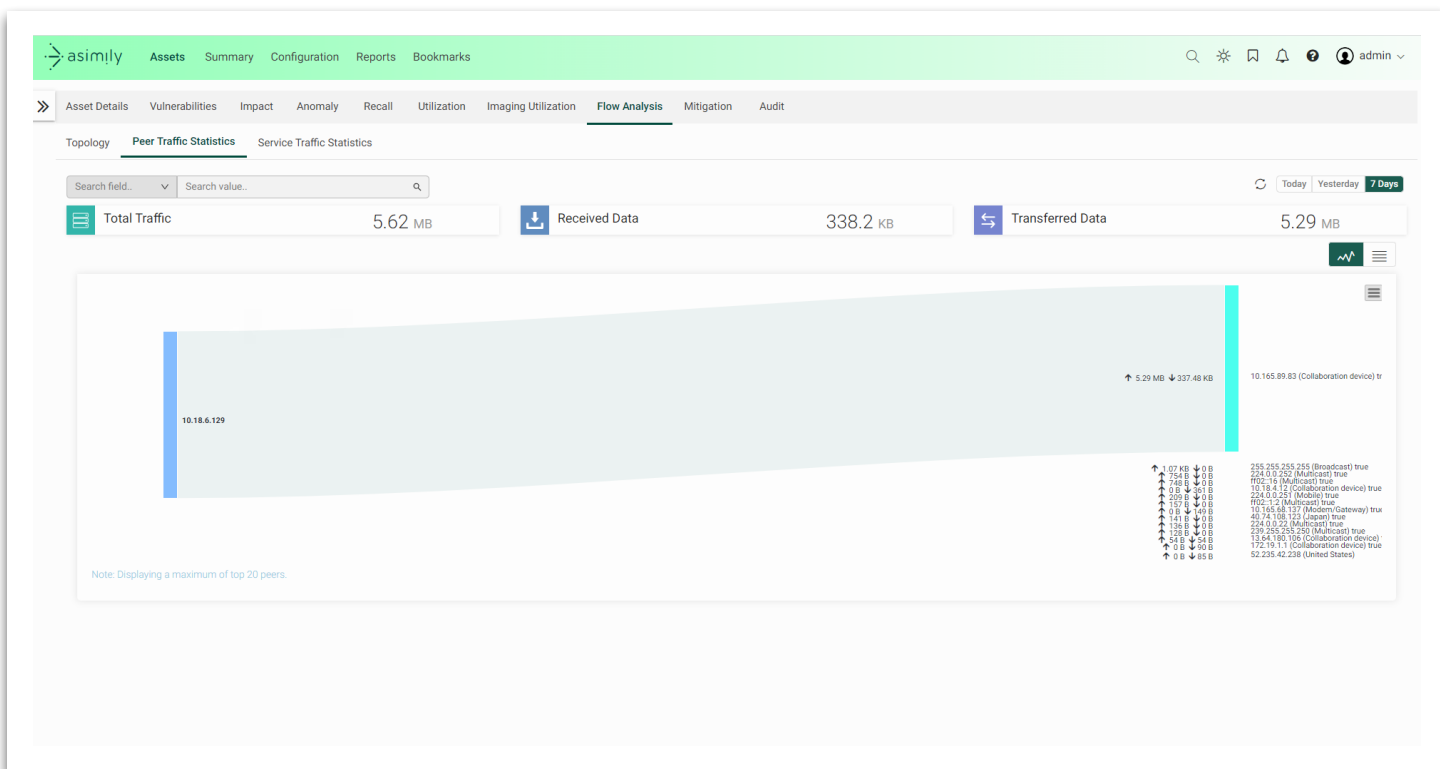
Incident Response (IR) and Forensic Analysis are expensive. IR services can easily cost millions of dollars per incident, depending on the scope of the investigation and the severity of the incident. Anywhere from 20% to 50% of this cost is taken up by data collection, including security logs, activity information, and other intelligence necessary for root cause analysis and other response activities. With the average attack cost of \$4.45 million per attack in 2023, this can be a significant cost.

Streamlining incident response and forensics is thus a critical component of a holistic approach to security and risk. Asimily's Policy Management enables you to track your supply chain by setting

detailed policies on any device, with any parameter in the network, to understand where your vendors could bring risk into the network. This then enables you to mitigate or act on it through our integrations. Understanding that supply chain and mitigating that risk is thus immensely valuable.

In terms of the cost of data collection, Asimily collects raw network captures from a device automatically at the time of the incident. As a result of this data collection capability, we cut the cost of data collection down to near zero for incident responders.

Flow Analysis Peer Traffic Statistics





Recover from Configuration Drift, Ransomware & More

A holistic approach to security needs to consider disaster recovery. Should the worst case happen, and a threat actor breaches critical systems and takes them down, there needs to be a plan in place for how to recover from that quickly. Computer systems need to be recovered, reimaged, or rebooted fast for companies to minimize loss and get back to work.

Configuration drifts are difficult to control at the best of times. If it were possible to keep configurations consistent and harden them, then around 90% of cybersecurity issues could likely be resolved. In the case of needing to remediate an issue, there is often a minimal record of what an IoT device looked like in a “good” state. Engineers typically reset these devices to factory settings when recovering from a disaster, but the optimal best state in practice is often a major unknown. This can be a major problem in terms of getting business operations back to normal, as it takes time in the field to reconfigure and recalibrate the device back to optimal conditions.

50%

of incidents caused by lack of talent

by 2025, lack of talent or human failure will be responsible for 50% of cyber incidents



To rectify this and accelerate the return to normal after a disaster, companies should baseline the optimal performance state with a snapshot to replicate device configurations. Having this snapshot can allow you to retain the golden state configuration, saving a tremendous amount of time and providing peace of mind. That way, if there are changes in the configuration

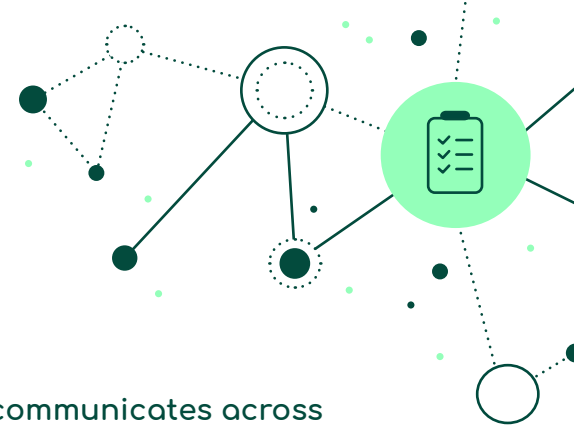
from a vendor breach or a manufacturer service representative accidentally making changes that they didn't realize affected security, the optimal state can be reverted to and easily resolved.

As part of ensuring an effective disaster recovery, security teams should monitor software updates and ensure they receive automated notifications for any configuration changes seen on the network. One of the risks of not knowing about this is that the update could reset the device and cause it to start communicating with an undesired external IP after the risk was remediated. This could be something as benign as sending information back to the manufacturer's IP address when previous configuration changes had stopped that.





Integrations Are Crucial for Better Risk Reduction



Integrating your security solutions into a cohesive whole that communicates across multiple dimensions is crucial for holistic security. IT and security teams should be able to access data across multiple solutions and dimensions for risk analysis, incident response, security triage, and more. A few of the solutions that you should make sure to integrate with and share information include:

CMMS, EAM & CMDB Integrations

Asimily integrates bidirectionally sync data between the CMMS, EAM, and CMDB systems - keeping them up-to-date when device attributes change and vice-versa. Depending on the integration target's support for it, Asimily can in some cases also automatically create work orders for issues like anomalies and vulnerabilities.

DHCP/IPAM Integrations

Integrating with DHCP/IPAM Systems enables Asimily to keep track of devices much better as they move across the network. This improves device classification and vulnerability assignment and is highly recommended for all customers.

Identity & Access Management (IAM) Integrations

IAM integrations enable Single Sign On (SSO), the ability to use your corporate username/password to log into Asimily.

ITSM Integrations

Asimily can automatically create tickets for issues including vulnerabilities, enabling easy tracking for critical fixes. Even if you primarily use a CMMS for medical device issue tracking, ITSM solutions may be useful for IoT devices that are not typically tracked in a CMMS.

Network Access Control (NAC) Integrations

NAC integrations can also be used to provide critical context, including device classifications and risk scores, to the NAC. This makes goals like automated segmentation based on device type much more achievable. Enrichment can be extremely useful for the IT/IS team even if they aren't Asimily users and do not want to apply policy via Asimily.

SIEM & SOC Integrations

Asimily can send anomaly event data to SIEMs in standard Syslog format, which can be handled by all major SIEMs. While you may not use a SIEM yourself, your SOC or IR team may be very interested in getting the context that Asimily anomaly alerts provide over other existing network security tools not designed or optimized for IoT.

Threat Intelligence Integrations

Asimily can ingest third-party threat intelligence if you subscribe to paid threat intel services. This threat intel will be displayed alongside Asimily's own assessment and anomaly alerts. Customers with their own threat intelligence services can add them to the over 100 sources used by Asimily for risk assessments and anomaly alerts.

Vulnerability Management (VM) Integrations

Asimily can use data from active scans to improve its vulnerability and OS identification. Asimily will also filter out irrelevant or non-attackable CVEs from those results, enabling much greater efficacy and efficiency than using VM scan results alone. Asimily can populate "no-scan lists" to ensure those devices are not inadvertently scanned, which can cause serious issues. Don't rely on fixed IP range exclusions – these are not reliable enough to ensure a lack of operational impact.

Integrating these tools, at least from a data-sharing perspective, ensures that you will have more complete access to insights across the system architecture. These integrations also create deeper efficiencies and can enable more automation to streamline your work even more. Much of this can be done with either APIs or native integrations, depending on the solutions that you select for your infrastructure.



Evaluate Risk Before Moving Forward

Any new software or new solution should be thoroughly evaluated from a risk management perspective before being connected to your systems. Risk assessments are a fantastic way to do this, and Asimily reduces the time to assess risk for a new perspective device through modeling connections to the network and automating device hardening recommendations. Normally, it takes anywhere from 6 to 8 hours to conduct a network impact analysis per device. Asimily has managed to reduce that to less than 1 to 2 hours per device through automation. Further, device risk emulation allows you to test different scenarios for the device in the network.

Risk evaluation needs to be done on a consistent basis as well. With the KPI benchmarking and reporting featured in the Asimily solution, organizations receive a simple-to-understand Org Risk Score that quantifies the level of risk incurred by your current security posture. Asimily provides executive risk reporting in the solution and MTTR tracking and benchmarking.



Asking for Budget



When asking for a budget to adopt a new security approach or solution, the first step is always to quantify the work you're already doing for risk remediation in your organization. This includes enumerating how many devices are in the environment, how many of them have vulnerabilities and risks, public data on how those vulnerabilities can be exploited, and how long it would take to fix them in the event of a crisis.

Once you've gotten that information collected, it should be compared to the number of hours that the organization would save by bringing an outsourced service provider on board. Make sure to include labor costs as part of your calculation, as this work needs to be done either by an external person or an internal person. If possible, supplement this data with an industry average risk score to further illuminate your security savings compared to the rest of the field. Merging individual data with the industry's average risk score highlights wider security risk trends and emphasizes how your company is doing in comparison.

Asimily Can Help

Unfortunately, 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 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 simplify recovery; and
- Our 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.](#)**

info@asimily.com
1-833-274-6459
Sunnyvale, CA
USA



About Asimily

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