THE RISKIEST CONNECTED DEVICES IN 2024

FORESCOUT RESEARCH | VEDERE LABS

June 10, 2024

CONTENTS

HOW WE QUANTIFY RISK IN DEVICES

To measure risk, we use a **multifactor risk scoring methodology** which is calculated based on three factors: Configuration, behavior and function.

- **CONFIGURATION** is the number and severity of vulnerabilities on a device, plus the quantity and criticality of open ports.
- **BEHAVIOR** tracks inbound and outbound malicious traffic to devices and inbound internet traffic towards the devices.
- **FUNCTION** is the potential impact to the organization if a device is compromised.

Each device is assigned a risk score between one and 10. After measuring the risk of each individual device, we calculate averages per type of device to understand which types are the riskiest.

For this report, we analyzed device data in Forescout's Device Cloud between January 1 and April 30.

1. Executive Summary

In 2024, attackers are crossing siloes to find entry points across the full spectrum of devices, operating systems and embedded firmware. Today, **network equipment has become the riskiest IT device category surpassing endpoints**. Threat actors are finding new vulnerabilities in routers and wireless access points — and are exploiting them quickly in massive campaigns. Similarly, **IoT devices with vulnerabilities expanded a whopping 136%** from a year ago.

And there is an emerging risky-device area to watch: **Industrial robots.** Special-purpose operating systems are also concerning: Our data shows **more than 2,500 unique versions to manage**.

Conversely, there is some positive news to report: **The healthcare industry's investment in device security is helping to reduce risk from a year ago.** In other positive vertical news, **nearly every industry reduced its Telnet exposure** and increased the use of SSH. However, healthcare is undoubtedly feeling the pain from major ransomware attacks in 2024, especially in the US. At the same time, the Internet of Medical Things (IoMT) has traded risk places with operational technology and moved up the risky-device scale.

Since 2021, we've recognized a persistent number of the usual risky-device suspects. For example, **programmable logic controllers (PLCs) and VoIP equipment are always on shaky ground**. They consistently make our risk list because this equipment is either inherently insecure or security protocols and configurations are ignored. It is incumbent on security leaders and teams to manage across these fragmented asset environments intelligently and with more control – even when activity is anomalous.

KEY FINDINGS

Forescout Research – Vedere Labs has been reporting on the riskiest devices in organizational networks using data sourced directly from nearly 19 million devices. This year marks our fourth annual report.

By Technology:

- IT devices account for most vulnerabilities (58%), down from 78% in 2023
- IoT vulnerabilities increased from 14% last year to 33% today (136% increase)
- The most vulnerable device types are:
  - Wireless access points
  - Routers
  - Printers
  - VoIP
  - IP cameras
- The most exposed unmanaged device types:
  - VoIP equipment
  - Networking equipment
  - Printers

By Vertical:

Top three with the riskiest devices:

- Technology
- Education
- Manufacturing

Healthcare had the biggest decline in risky devices this year by reducing:

- RDP use
- Legacy Windows version use

Highest percentage of legacy Windows versions found:

- Technology
- Education
- Retail
- Healthcare

2. Riskiest Connected Devices in 2024

Using our dataset and scoring methodology, we identified the five riskiest device types in four device categories: IT, IoT, OT and IoMT

Table 1 – Riskiest connected devices per category

IT	IoT	OT	IoMT
Router	Network attached storage (NAS)	Uninterruptible power supply (UPS)	Medical information system
Wireless Access Point	VoIP	Distributed control systems (DCS)	Electrocardiograph
Server	IP camera	Programmable logic controller (PLC)	DICOM workstation
Computer	Network Video Recorder	Robotics	Picture archiving and communication system (PACS)
Hypervisor	Printer	Building management system (BMS)	Medication dispensing system

*blue highlight represents the nine device types not included in the 2023 Riskiest Devices report

Out of these 20 device types, 11 were included in the 2023 report and remain on the list. **Nine device types were not in the 2023 list** (highlighted in blue on the table): Wireless access point, hypervisor, NVR, robotics and all the devices in the IoMT category. Out of these nine, four were in the 2022 list and returned. Yet, four are completely new: NVR, robotics, medical information system, electrocardiograph and medication dispensing system.

IT devices

The riskiest IT devices continue to be divided into two main groups: Network infrastructure devices and endpoints.

Network infrastructure devices – routers and wireless access points – are often exposed online and have dangerous open ports. At the beginning of 2023 endpoints were still riskier than network devices. Today, we see a reversal **which represents an increase in the number of vulnerabilities found and exploited in network infrastructure devices since the second half of 2023.**

Routers are much more often exploited remotely but wireless access points are the typical border between internal and external networks in physical locations. They frequently host guest and corporate networks and are used to connect guest devices, including computers and mobile.

Endpoints – servers, computers and hypervisors – remain risky for being the entry points for phishing or because of unpatched systems and applications. Additionally, hypervisors**,** or specialized servers hosting virtual machines (VMs) have become a favorite target for ransomware gangs since 2022 because they allow attackers to encrypt several VMs at once.

Ransomware developers are moving towards languages, such as Go and Rust, that allow for easier cross-compilation and can target Linux *and* Windows. Just like network infrastructure devices, hypervisors are typically unmanaged and do not support traditional endpoint protection agents.

IoT devices

The riskiest IoT devices include the most persistent suspects – NAS, VoIP, IP cameras and printers. These are commonly exposed on the internet and have been historically targeted by attackers. However, there is one new entry: NVR.

NAS devices have been a growing target for ransomware actors with several ransomware families designed specifically to run on them due to the valuable data they store and their numerous vulnerabilities.

VoIP and IP cameras are risky because they are commonly exposed on the internet and there is a long history of threat actors targeting them. In 2019, APT28 compromised VoIP phones for initial access to multiple networks. In 2021 Conti targeted cameras to move internally in affected organizations. In 2022, APT29 and TAG-38 targeted cameras for use as command and control infrastructure.

NVRs sit alongside IP cameras on a network to store their recorded video. Just like IP cameras, they are commonly found online and have significant vulnerabilities that have been exploited by cybercriminal botnets and APTs.

Printers include multifunctional printing and copying devices used in the connected office. They also include specialized devices for printing receipts, labels, tickets, wristbands and other uses. Although printers are not widely associated with cyber risk, they should be. Like IP cameras, they have been exploited by threat actors, such as APT28 and spammed by hacktivists on multiple occasions. Printers are also often connected to sensitive devices, such as point of sales systems and conventional workstations with privileged users.

OT devices

The riskiest OT devices include the critical and insecure-by-design PLCs and DCSs. It also includes the UPSs present in many data centers with default credentials — and the ubiquitous, often invisible building automation systems.

UPSs play a critical role in power monitoring and data center power management. CISA has alerted about threat actors targeting UPSs with default credentials. Attacks on these devices can have physical effects, such as switching off the power in a critical location or tampering with voltage to damage sensitive equipment.

PLCs and DCSs are risky because they are very critical, allowing for full control of industrial processes, and are known to be insecure by design, often allowing attackers to interact with them and even reconfigure them without the need for authentication.

Building management systems, also known as building automation systems, are critical for facilities management. There are several examples of smart buildings exploited by threat actors to render controllers unusable, recruit vulnerable physical access control devices for botnets, or leverage management workstations for initial access. These devices dangerously mix the insecure-by-design nature of OT with the internet connectivity of IoT and are often found exposed online even in critical locations.

Robotics: The use of robots is quickly increasing in industries, such as electronics and automotive manufacturing, where factories are becoming 'smarter' and more connected. There were close to 4 million industrial robots worldwide in 2023 with around 80% in just five countries: China, Japan, US, South Korea and Germany.

There are also service robots deployed in a variety of other industries, such as logistics and the military. Despite popular use, many robots have the same security issues as other OT equipment, including: outdated

software, default credentials and lax security postures. Attacks on robots range from production sabotage to physical damage and human safety.

IoMT devices

The riskiest IoMT devices have all changed from last year, but they include a mix of IT equipment used for healthcare, such as medical information systems and workstations. These systems often have dedicated embedded devices, such as electrocardiographs and automated medication dispensing.

Medical information systems store and manage clinical data using standard formats such as HL7 to connect systems containing, for instance, electronic health records and billing information. These systems store very sensitive information which is valuable on the dark web and are often leaked by ransomware gangs. Despite the criticality of their data, thousands of these systems can still be found exposed online.

Electrocardiographs are risky because of their fundamental role and large impact in acute patient care. A peer-reviewed study showed that data breach remediation efforts in hospitals led to a 2.7 minute delay in performing ECGs, thus increasing patient mortality by 0.36%. As the authors indicated, that could be even worse in the case of ransomware incidents (which was not part of their dataset). On our dataset, electrocardiographs were the third most vulnerable IoMT device, after medication dispensing systems and infusion pumps**.**

DICOM workstations and PACS are used in medical imaging. They often run legacy vulnerable IT operating systems, have extensive network connectivity to allow for sharing imaging files and use the DICOM standard for sharing these files. DICOM defines the format for storing medical images *and* the communication protocol used to exchange them. The protocol supports message encryption, but its usage is configured by individual healthcare organizations. **We observe unencrypted communications in many organizations, which could allow attackers to obtain or tamper with medical images, including to spread malware.** PACS are by far the most commonly exposed IoMT device in our dataset.

Medication dispensing systems have been known to be vulnerable for almost a decade, since Billy Rios documented 1,418 vulnerabilities on seven third-party components of a popular device in this category. More than eight years after that study, we still see medication dispensing systems as the sixth most vulnerable device type overall, not just in the IoMT category (see section 3.5).

There are documented cases of ransomware attacks affecting the availability of dispensing systems, which can cause delays in patient treatment. **We also reported on 183 of these systems exposed online in 2022. Less than 2 years later, that number has grown to 225. Medication dispensing systems are the second most exposed IoMT device type in our dataset.**

3. Detailed Analysis

3.1. Risk by industry

Figure 1 shows the distribution of average device risk by industry in our dataset. We selected the 10 industries with the most devices for this analysis.

In 2024, technology has the riskiest devices on average, followed by education and manufacturing. We changed the sorting methodology from last year when we counted the percentage of devices with critical or high risk, rather than average risk across devices.

Healthcare has made notable strides and is no longer the riskiest industry. Last year, it had the largest percentage of high and medium risk devices. Today, it average device risk is 7.25 — the lowest of the 10 industries. Similarly, retail was the second riskiest in 2023 and has also shown a big improvement this year.

Retail now ranks just above healthcare at 7.37 average device risk. Manufacturing remains the third riskiest at 7.98.

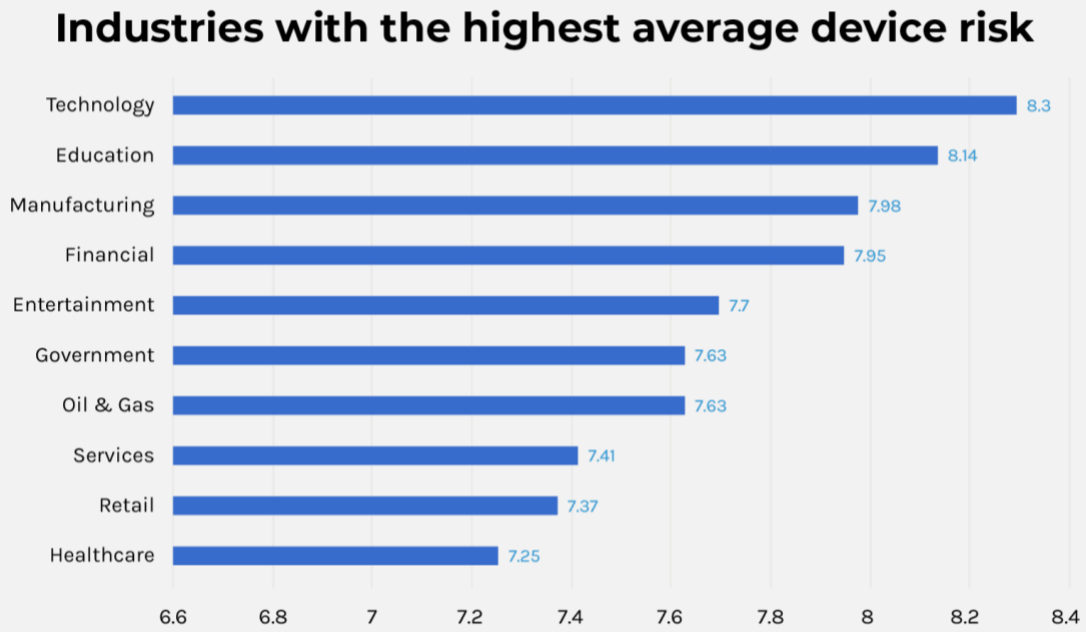

Figure 1 – Industries with the highest average device risk

3.2. Risk by country

Figure 2 shows the distribution of average device risk by country. We selected the 13 countries that had an average device risk greater than 6.0. The top three countries with the riskiest devices on average are all in Asia. They are followed by Canada and the US. The riskiest European countries are Denmark, Italy and the UK.

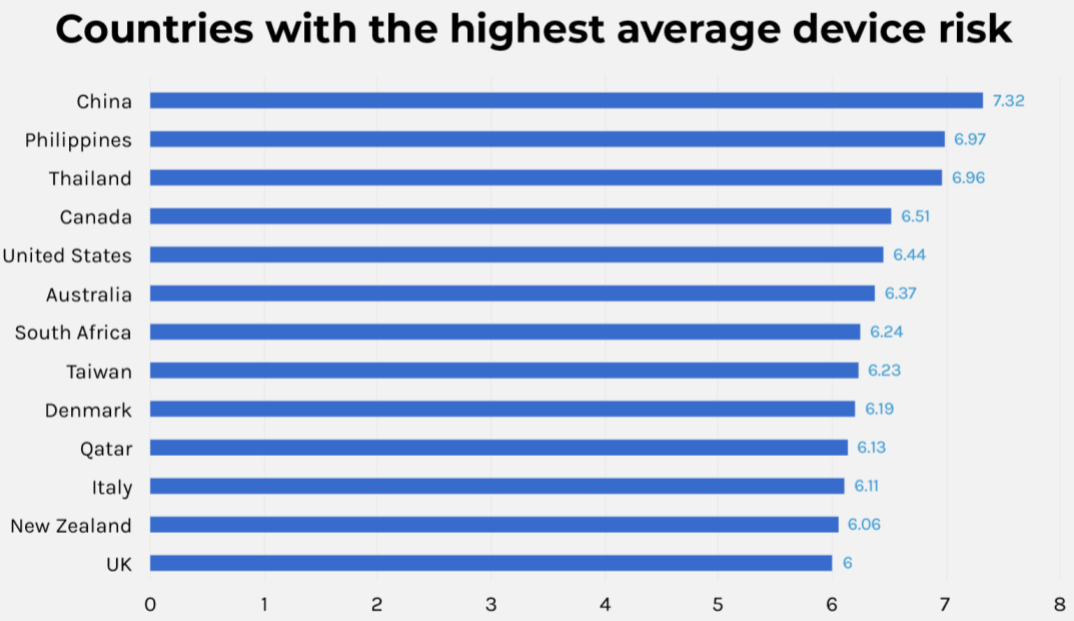

Figure 2 – Countries with the highest average device risk

3.3. Operating systems

Figure 3 shows the operating systems (OS) of devices across the 10 industries. Most devices still run 'traditional' IT OSes, such as Windows, Linux, Mac and UNIX. This includes several specialized IoT/OT/IoMT devices that run Linux or Windows. However, the category of special purpose OSes is particularly strong in oil and gas (21%), healthcare and entertainment (14% each) and retail (12%). Special purpose OSes are more common than mobile OSes in all industries except education.

The variety of special purpose OSes is a nightmare for security teams to keep track of and is one of the main reasons for more visibility into networked devices. We observe more than 2,500 unique versions on the Device Cloud. Embedded firmware is also well known for presenting systematic security issues, such as backdoors, hardcoded credentials and keys and memory corruption vulnerabilities.

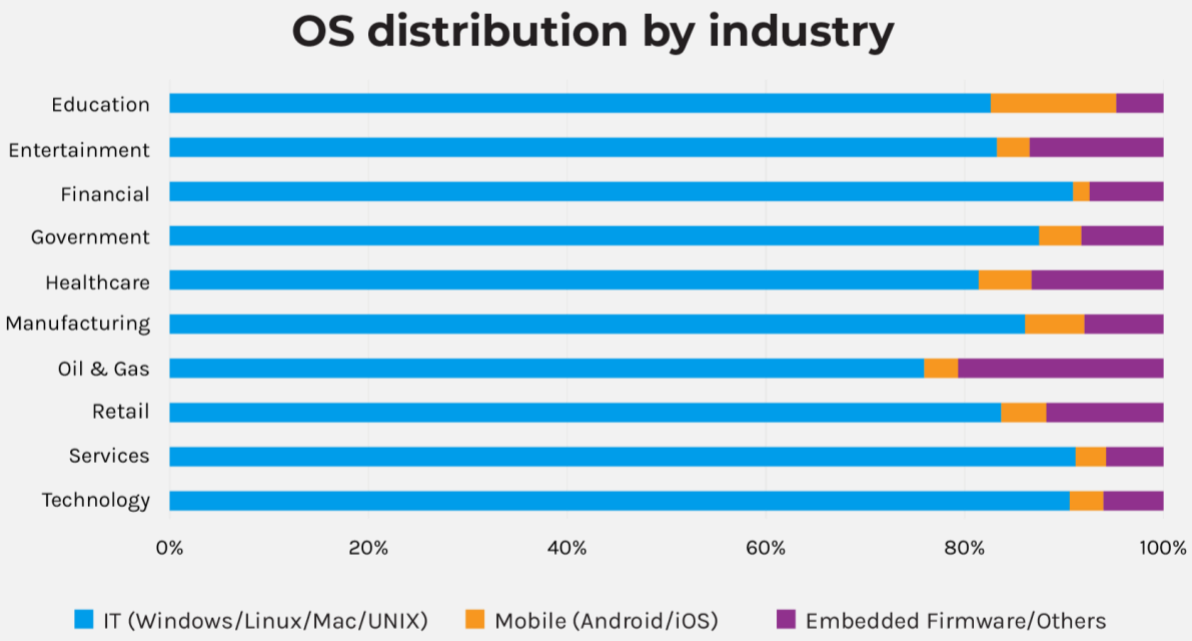

Figure 3 – OS distribution by industry

Since Windows is by far the most common operating system across every industry, we drill down into the versions used in each industry. We divide Windows versions into two categories: currently supported – such as Windows 10 and 11 – and legacy, which includes versions such as Windows 8, 7, XP and CE.

Figure 4 shows the percentage of devices running legacy Windows versions in each industry. Technology has the highest percentage with 6% of devices, education comes second with 5%, followed by retail and healthcare with 4% each.

In 2023, we only reported legacy Windows devices for five industries – financial, government, healthcare, manufacturing and retail – but all those industries showed a significant decrease in the percentage of legacy versions in 2024. The highest drop was in healthcare which decreased from 6% to 4% — which highlights that the security efforts of healthcare organizations are having a positive impact.

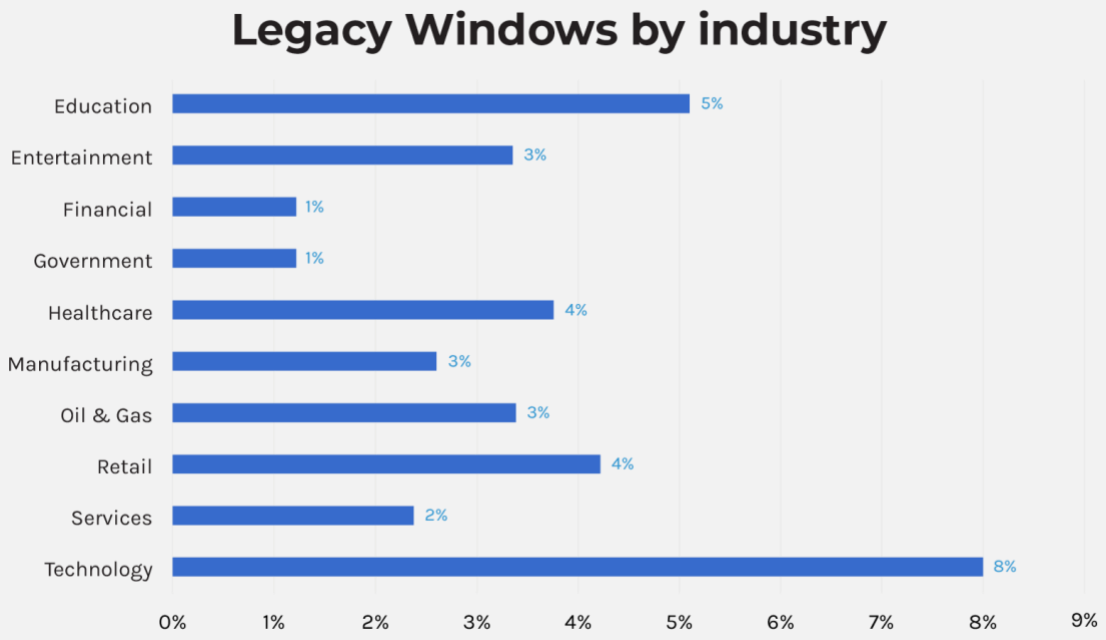

Figure 4 – Legacy Windows by industry

3.4. Vulnerabilities

Figure 5 shows the device categories most often found vulnerable. IT devices still account for most vulnerabilities (58%), but that is down from 78% in 2023. IoT vulnerabilities increased from 14% last year to 33% now. Last year, there were more OT vulnerabilities than IoMT, but this year the ranking is reversed with IoMT in third (5%) and OT in fourth (4%).

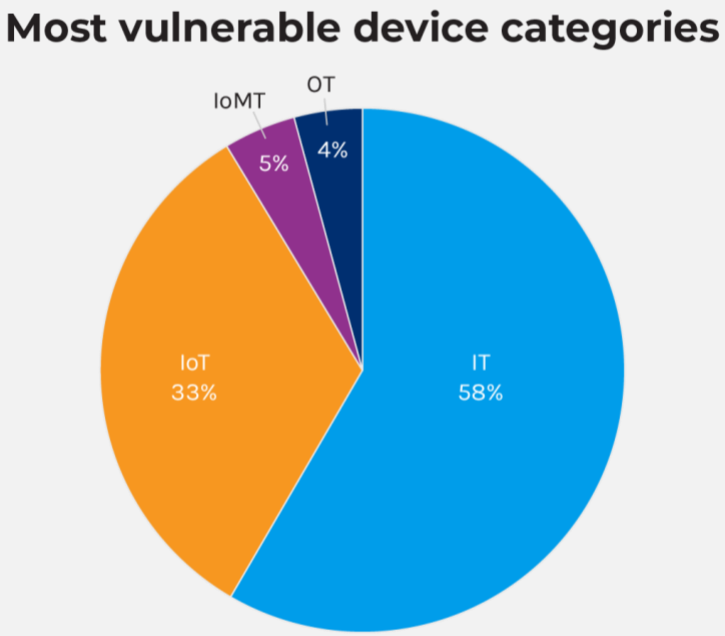

Figure 5 – Most vulnerable device categories

Figure 6 shows the device types most often found vulnerable. Not surprisingly, seven of these top 10 are among the riskiest devices shown in Table 1, since vulnerabilities are one of the top risk factors for devices.

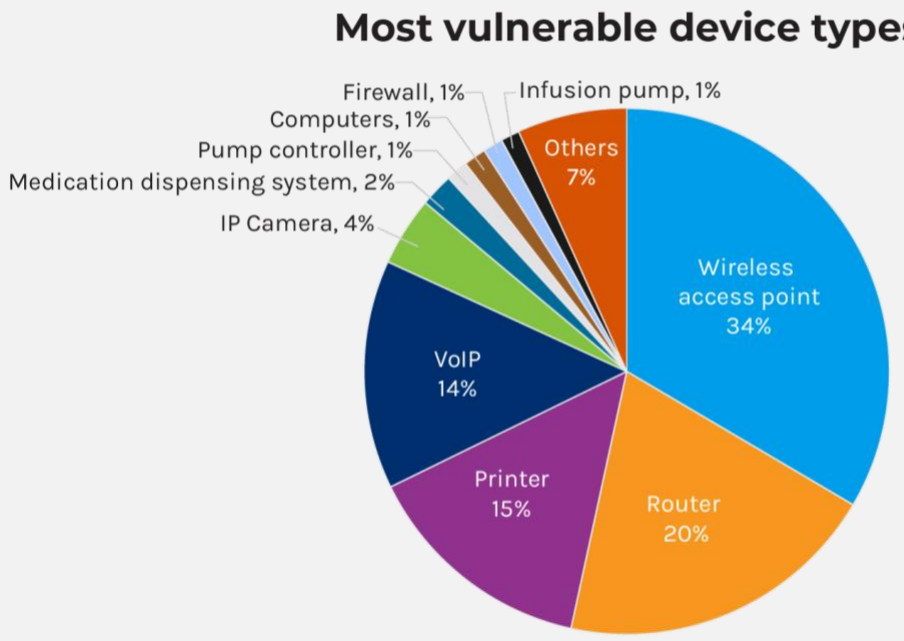

Figure 6 – Most vulnerable device types

3.5. Open ports

Vulnerabilities are a major risk factor for devices, but open ports are what leave devices open to attacks. We selected four common ports to analyze out of the ones we observed as most exploited in 2023. Server Message Block Protocol (SMB) is used by Windows machines for file sharing, printer sharing and access to remote services. Remote Desktop Protocol (RDP) provides remote management for devices using a graphical interface. Secure Shell (SSH) provides remote management using a command-line interface especially to Linux/UNIX servers and IoT devices, while Telnet also provides remote management mainly for legacy specialized devices.

Figure 7 shows the percentage of devices in each industry with a given open port. SMB and SSH are the most popular protocols, followed by RDP and Telnet. The most Telnet devices are found in healthcare (4%), technology (3%) and manufacturing (3%). The most SSH are found in entertainment (52%), technology (39%) and oil and gas (33%). The most RDP are found in services (14%), oil and gas (12%) and manufacturing (12%). The most SMB is found in technology (37%), financial (32%) and services (30%).

Compared to 2023, we see that every industry we tracked last year reduced its Telnet exposure, except for manufacturing where it remained stable at 3%. The highest Telnet decrease was in healthcare which moved from 10% to 4%. On the other hand, SSH increased in every industry. This may be an indication that organizations are replacing remote management of devices via Telnet with SSH which is a good sign. RDP also decreased in every industry, except for manufacturing. Once again, the highest decrease was in healthcare, from 16% to 6%. SMB had a mixed result, with government, healthcare and retail reducing exposure but financial and manufacturing increased slightly.

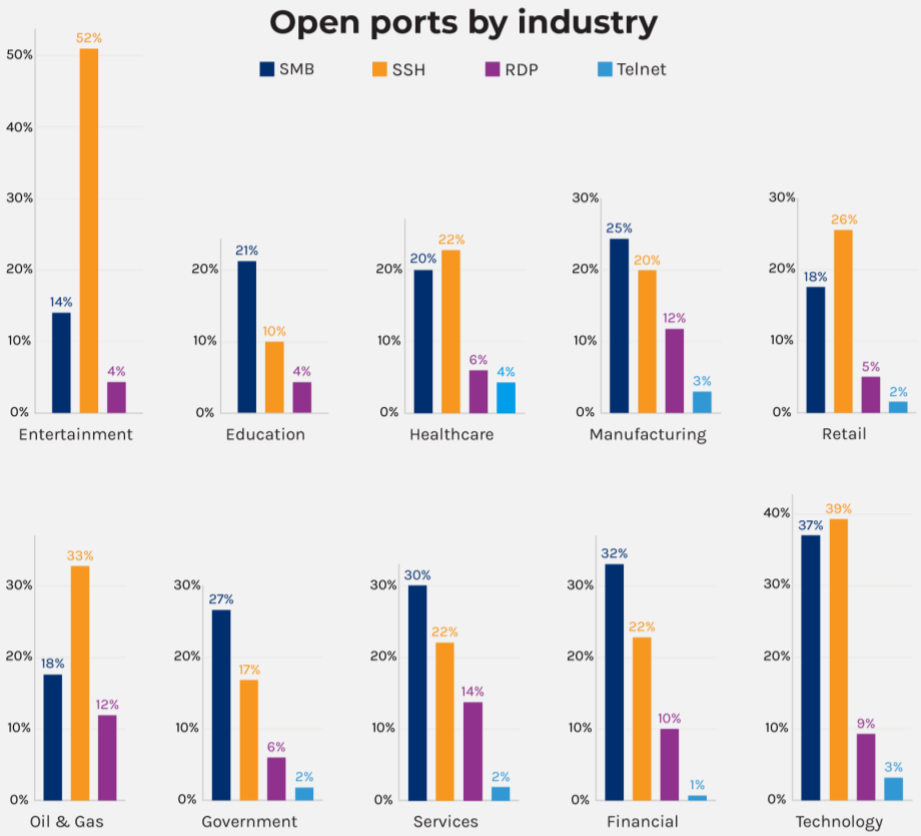

Figure 7 – Open ports by industry

3.6. Internet exposure

Figure 8 shows the most often exposed device types. Computers, mobile and servers represent nearly 90% of the exposed devices. The most exposed unmanaged device types includes VoIP equipment (5%), networking equipment (3%) and printers (1%) . The 'other IoT' group includes more than 30 other types of commonly exposed IoT devices. The majority are IP cameras, smart TVs and NAS. 'Other IoMT' includes over 40 types of IoMT devices, including PACS systems, blood glucose meters and healthcare workstations. Finally, 'other OT' includes 20 types of devices, such as UPS, PLC and building automation systems.

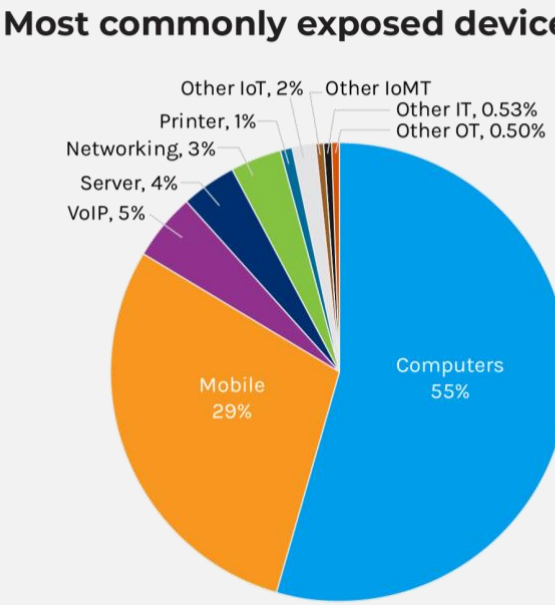

Figure 8 – Most commonly exposed device types

4. Conclusion

The attack surface now encompasses IT, IoT and OT in almost every organization — with IoMT in healthcare. It is not enough to focus defenses on risky devices in a single category since attackers can leverage devices of different categories to carry out attacks. We have demonstrated this with, a proof-of-concept attack (R4IoT) that starts with an IP camera (IoT), moves to a workstation (IT) and disables PLCs (OT).

To defend this expanded attack surface, organizations need new security approaches to identify and reduce risk. As the threat landscape continues to evolve and more organizations adopt cybersecurity only for traditional endpoints, threat actors are consistently moving to devices that offer easier initial access.

Modern risk and exposure management must encompass devices in every category to identify, prioritize and reduce risk across the whole organization. Solutions that work only for specific devices cannot effectively reduce risk because they are blind to other parts of the network being leveraged for an attack. For example, IoMT-only solutions will not effectively assess risk for IT devices. At the same time, IT-only solutions will miss the nuances of specialized devices.

Beyond risk assessment, risk mitigation should use automated controls that do not rely only on security agents but apply to the whole enterprise, not individual siloes.