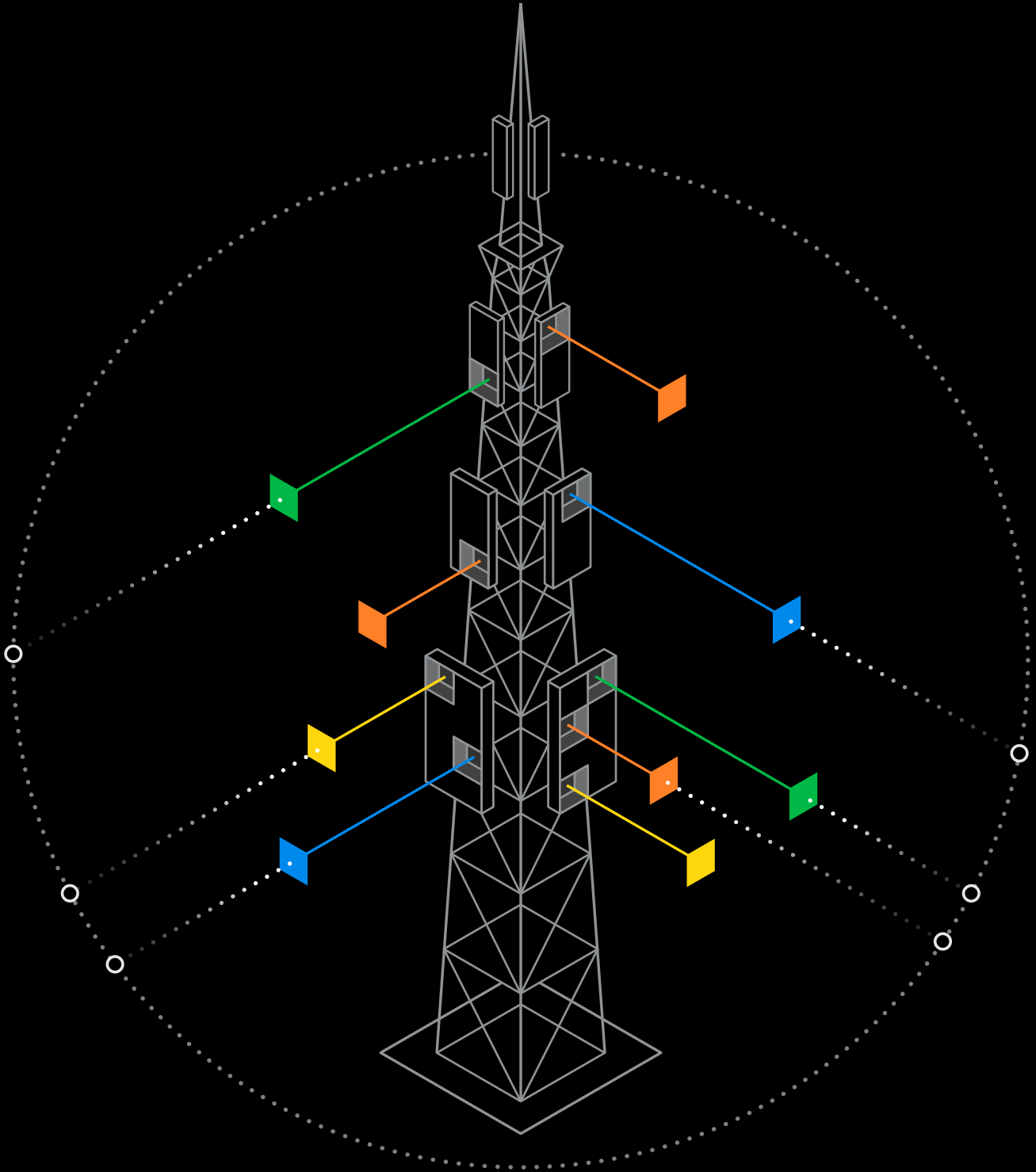


# 2024 Mobile Security Index



## **Who should read this report?**

We produced the Verizon Mobile Security Index (MSI) to help security professionals, such as chief information security officers (CISOs), assess their organization's mobile security environment and calibrate their defenses. This report is also relevant to anybody involved in the specification, procurement or management of IT devices and services.

## **About this report**

In April 2024, we commissioned an independent market research company to survey 600 people responsible for security strategy, policy and management. We also worked with several leaders in mobile device security: Akamai, Allot, CISCO, Fortinet, Ivanti, Jamf and Lookout. These contributors provided additional information, including incident and usage data.

We'd like to thank all our contributors for helping us to present a more complete picture of the threats that affect mobile devices and the work that is being done to mitigate these threats. This report wouldn't be possible without them.

For more information on our methodology, see page 45.

## **About the cover**

The depiction of a cell tower on the cover reflects mobile device security issues in critical infrastructure sectors that were seen in this year's MSI survey responses. Critical infrastructure industries supply the essentials of daily life to millions, including power, water, communications and transportation. In parallel, there are heightened risks from threat actors targeting organizations in these industries, along with an expanding attack surface from increasing Internet of Things (IoT) and mobile device use. Enhancing mobile device security serves to reduce financial and operational risks for organizations in all industries. In critical infrastructure, it has even more profound implications.

# Table of contents

<b>Introduction – critical infrastructure on the radar</b>	<b>4</b>
<b>Modern work, enabled by mobile</b>	<b>5</b>
<b>IoT – everything, everywhere, all at once</b>	<b>7</b>
<b>IoT use is especially high in critical infrastructure sectors.</b>	<b>9</b>
<b>IoT security risks: Amplified in critical infrastructure sectors</b>	<b>12</b>
<b>All sectors perceive increased mobile and IoT risk.</b>	<b>14</b>
<b>Breach risks and impacts are high, especially in critical infrastructure.</b>	<b>18</b>
<b>Shadow IT: A looming security challenge</b>	<b>21</b>
<b>Emerging AI cyberthreats meet new AI defenses.</b>	<b>25</b>
<b>The disconnect between perceived and actual mobile security</b>	<b>26</b>
<b>Critical infrastructure sectors have specific considerations.</b>	<b>29</b>
<b>Mobile security awareness and solution investments are rising.</b>	<b>34</b>
<b>IoT security is also making strides.</b>	<b>37</b>
<b>But IoT security gaps remain.</b>	<b>38</b>
<b>More to do. More that can be done.</b>	<b>40</b>
<b>The call to arms: Move faster.</b>	<b>43</b>
<b>Survey methodology</b>	<b>45</b>
<b>Contributors</b>	<b>46</b>

# Critical infrastructure on the radar

**The first iPhone was released in 2007. Mobile devices have evolved dramatically and are now embedded into the daily lives of billions of people around the globe. What's more, the already healthy use of mobile devices by organizations and their employees shot into the stratosphere during the COVID-19 pandemic, when remote work suddenly became the new normal and kitchens and living rooms were instantly transformed into remote offices.**

This 2024 Verizon Mobile Security Index report has some familiar themes—such as the persistence of remote and hybrid work—while also revealing emerging mobile security considerations relating to critical infrastructure sectors, rising Internet of Things (IoT) deployments and artificial intelligence (AI) advances (from both attack and defense perspectives). We also found interesting differences between respondents' perceptions and reality. Many assume that they had solid mobile security in place and that incident remediation would be quick and easy. But what those respondents actually report about attacks and breach frequency, along with negative breach impacts and worries, told a different story.

In our deeper dive into the critical infrastructure sector, we found that inadequate mobile security in any of the 16 defined critical infrastructure industries could have significant impacts on organizations in these industries and could have downstream impacts on the communities and individuals served.

From the survey data, one primary conclusion can be drawn: The growth of mobile computing and IoT is exponentially expanding the attack surface that needs protection, which in turn will require a matching focus on ensuring sufficient mobile security processes, policies and investments.

# Modern work, enabled by mobile

Even as some organizations pull workers back to the office, the remote or hybrid work paradigm is not likely to shift back to its prior state anytime soon. One reason is employees still strongly prefer the flexibility to work remotely at least some of the time, to work non-traditional hours, or to spend part of each workday in the office and part at home.

92%

of office-based employees value being able to work flexible hours.<sup>1</sup>

92%

of organizations have employees who work from home at least some of the time.

89%

value working remotely at least part time.<sup>2</sup>

83%

have employees who follow a hybrid work model.

90%

value being able to leave work during the day for personal reasons.<sup>3</sup>

80%

have employees who travel for work.

**Employers on the whole still favor allowing employees to work remotely. Whether it's working from home, the airport, a hotel or the local coffee shop, 92% of survey respondents say their organizations support some form of remote connectivity. This means that mobile devices are more deeply embedded into business-critical workflows than they were in the past.**

80%

of respondents agree mobile devices are critical to the smooth running of their organizations.

55%

of organizations have more users with more mobile devices than they did 12 months ago.

46%

of respondents agree that mobile devices have gone from a nice to have to a critical business tool.

1 Ivanti, Everywhere Work Report, 2024.

2 Ibid.

3 Ibid.

Employer support for flexible and remote work means an expanding array of mobile devices of various types are connecting to enterprise networks on a regular basis.

Increasingly, these devices are also being used to access sensitive information.

**50%**

**say mobile devices have greater access to sensitive information than a year ago.**

**86%**

**agree that flexibility in where people work and what devices they use is key for attracting top talent.**

**86%**

**agree that increased remote working has moved mobile security up their agenda.**



**Because mobile devices now play an ever-expanding role in enterprise computing environments, these ecosystems are more complex, more diverse and more dynamic than ever before.**

**62%**

**of authentications to corporate networks come from mobile and non-traditional operating systems—a new high.<sup>4</sup>**

**With hybrid and remote work becoming an established cornerstone of workplace policy and organizations depending more heavily on more different types of devices—in more locations—strategic investments in mobile security are no longer optional.**

<sup>4</sup> Cisco, Duo Trusted Access Report, 2024.

# IoT—everything, everywhere, all at once

Mobile devices have been keeping businesses up and running for years. What's changed recently is rapid growth in IoT deployments. These “things” give real-time visibility into the status of thousands of processes, from how machines are performing in factories to where vehicle fleets are traveling each day—even whether office buildings are set to the right temperature.

IoT adoption supports digital transformation across nearly every industry, making it possible to keep a watchful eye on the performance of key assets and enabling smarter, data-driven decisions.

## More IoT devices than ever

While reliance on mobile devices across all types of organizations has remained high, increasing only slightly over the last few years, IoT use has become nearly as ubiquitous. Nearly all organizations are using at least some IoT devices. What's more, the majority of deployments are mature, full-scale implementations, not partial deployments or proofs-of-concept.

95%

**of survey respondents  
work for organizations  
that are using at least  
some IoT devices.**

62%

**said they have mature,  
full-scale IoT deployments.**

# Nearly infinite applications and use cases

IoT sensors and devices are being applied in an enormous and expanding array of use cases. They're helping keep facilities secure and comfortable, hospital patients properly monitored and cared for, and supply chains flowing. Retailers use them to track store inventories, while others use IoT to monitor energy consumption. Another popular use case is predictive maintenance, which supports more reliable uptime in production operations, such as those in the manufacturing or energy sectors.

Organizations that use IoT devices are using them in more than three ways, on average.

## Use of IoT sensors or devices

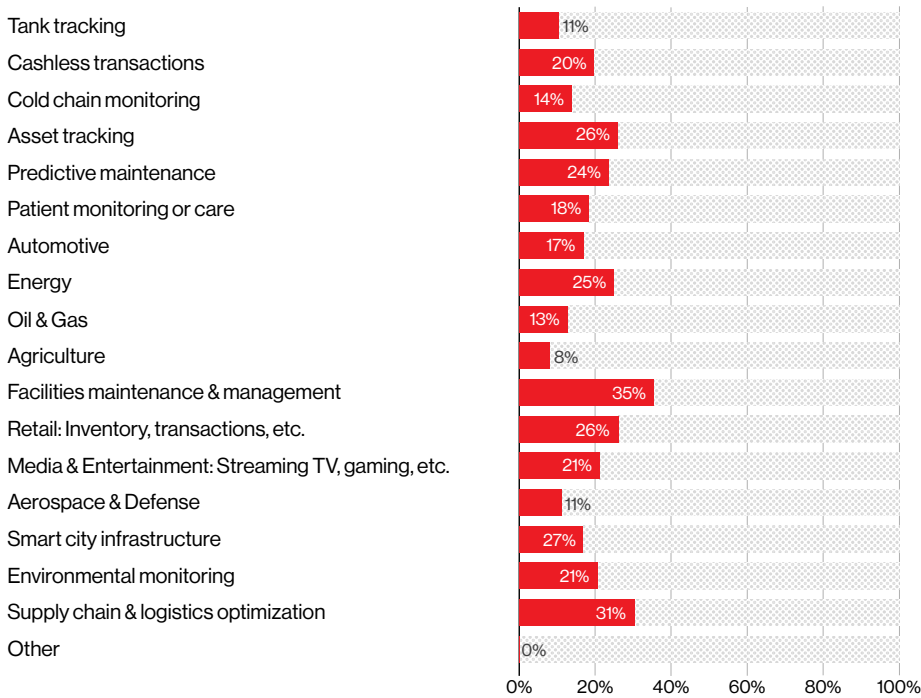


Figure 1



# IoT use is especially high in critical infrastructure sectors.

The National Institute of Standards and Technology (NIST) describes critical infrastructure industries as providing a “backbone for society’s economy, security and health.”<sup>5</sup>

As such, these sectors are often a prime target of nation-state threat actors according to NIST, especially those focused on disrupting national security and public safety—because critical infrastructure operations are considered essential to national security.

Today, the widespread and growing use of IoT sensors and internet-connected devices can also expand cyber risks.

## The many uses of IoT in critical infrastructure

IoT devices and sensors today are used to monitor and control all types of assets, facilities and systems across a wide range of critical processes, increasing efficiency, security and resilience. IoT devices enable predictive maintenance across industrial environments and can detect an early-stage equipment failure before it results in downtime. They are also used to improve worker safety while decreasing the need for manual interventions.

IoT devices are also used to transform power supply networks into smart grids, turning metropolitan areas into smart cities, and making many types of public facilities safer and more comfortable. And that’s just the tip of the iceberg of IoT uses across critical infrastructure operations.

As a result, IoT adoption is expanding rapidly across nearly all critical infrastructure sectors.

96%

of critical infrastructure organizations report some degree of IoT adoption.

## What is critical infrastructure?

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has designated 16 industries as critical infrastructure sectors, as follows.<sup>6</sup>

- **Chemical**—enterprises that manufacture, store, use and transport chemicals, including potentially dangerous chemicals on which other sectors rely
- **Commercial facilities**—sites where large crowds of people gather for shopping, business, entertainment or other activities
- **Communications**—an interoperable network of satellites, wireless and wireline communications that provides an enabling function across all critical infrastructure sectors
- **Critical manufacturing**—a subset of manufacturing with national significance, for which a successful attack could disrupt essential functions at a national level

(Cont.)

5 National Institute of Standards and Technology (NIST), Special Publication (SP) 800-175A, 2016.

6 Cybersecurity and Infrastructure Security Agency (CISA), Critical Infrastructure Sectors.

**Across all critical infrastructure sectors, respondents from energy utilities and Public Sector organizations report the most IoT projects in production.**

Is your organization using IoT devices?

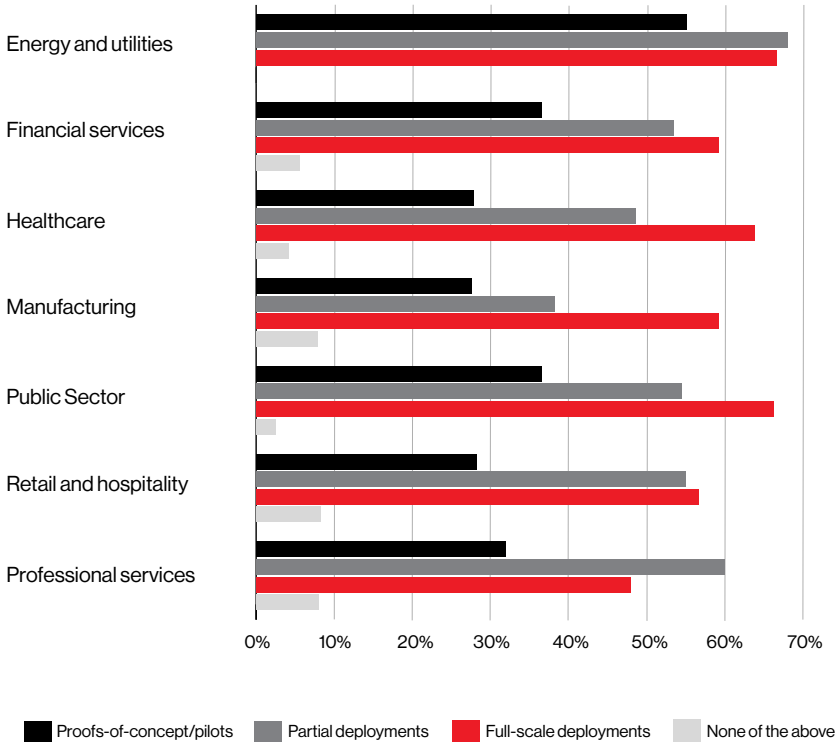


Figure 2

- **Dams**—critical water retention and control services, including hydroelectric power generation, municipal and industrial water supplies and agricultural irrigation
- **Defense industrial base (DIB)**—the worldwide industrial complex that enables the research and development of military weapons systems, subsystems and components
- **Emergency services**—resources that provide a range of prevention, preparedness, response and recovery services to help save lives and protect property and the environment
- **Energy**—a multifaceted web of electricity, oil and natural gas resources and assets that also provides an enabling function across all critical infrastructure sectors
- **Financial services**—the large global firms, nationwide and community banks, and credit unions that make it possible for consumers to deposit and invest funds, make payments, access credit and liquidity, and transfer financial risks
- **Food and agriculture**—farms and restaurants, as well as food manufacturing, processing and storage facilities
- **Government facilities**—a wide variety of buildings in the U.S. and abroad, many of which are open to the public that are owned or leased by federal, state, local and/or tribal governments

(Cont.)

**These projects deliver value across an array of use cases, including physical security, environmental monitoring, location tracking and telehealth, among others.**

**61%**

**of critical infrastructure respondents use IoT devices to monitor the physical security of buildings and other properties, including video surveillance.**

**52%**

**of critical infrastructure respondents use IoT devices to support efficiency by monitoring equipment or productivity.**

**52%**

**of critical infrastructure respondents use IoT devices to enable services such as digital signage, or to support consumer offerings such as wearables or in-vehicle services.**



- **Healthcare and public health** – focuses on population health and provides the response and recovery actions needed after large-scale hazards such as terrorism, infectious disease and natural disasters
- **Information technology** – virtual and distributed functions that produce and deliver hardware, software, systems and services that help enable internet connectivity
- **Nuclear reactors, materials and waste** – the nuclear power plants, research and test reactors, fuel cycle facilities, and waste management systems that help make up America’s extensive civilian nuclear infrastructure
- **Transportation systems** – the modes such as aviation, trucking, maritime, rail, pipelines, postal/shipping services and mass transit that move people and goods across the country and overseas
- **Water and wastewater** – the systems that provide safe drinking water and wastewater treatment services

# IoT security risks: Amplified in critical infrastructure sectors

**IoT devices often have weak security and network connectivity. This makes their existence an expansion of the attack surface. This exposure is particularly concerning for critical infrastructure organizations, which are already attractive targets for some of the most sophisticated and best-resourced threat actors in the world.**

IoT devices are still not subject to asset management or security monitoring in all organizations. And IoT devices tend to monitor legacy equipment in operational technology (OT) environments that may lack modern security features—a common reality in critical infrastructure industries.

## IoT vulnerabilities

Many IoT security vulnerabilities exist from the time of the device's manufacture. Many come with weak default passwords, and changing them often isn't intuitive. Some devices have credentials embedded in firmware, making them impossible to change. Others may not use authentication at all. And because IoT devices are designed to use little power to reduce costs and extend battery life, their processing capabilities are extremely limited. This limitation means they can't run anti-malware programs or encrypt data shared across enterprise networks.

Network connectivity dominates IoT security challenges. Many devices are designed to connect automatically to the nearest Wi-Fi or local area network (LAN), potentially turning each device into an easy and attractive entry point for attackers looking for a stepping stone to wider networks.

At the same time, it can be difficult to secure communications between IoT devices and cloud apps. And it's also often hard to deliver and install security updates to devices in the field.

A lack of industrywide security standards for IoT devices and their communication protocols increases security risks, as does having many devices installed in remote locations where they may be vulnerable to physical tampering.

## Critical infrastructure on the radar

IoT adoption is widespread in critical infrastructure sectors, where nearly all respondents report that they have at least some IoT devices in use.

More than half of respondents in critical infrastructure sectors report that they had experienced significant security incidents involving mobile or IoT devices. By "significant security incidents," we mean incidents resulting in data loss or system downtime.

96%

**of critical infrastructure organizations use IoT devices.**

53%

**of critical infrastructure respondents have experienced significant mobile or IoT device-related security incidents leading to data loss or system downtime.**

48%

**of critical infrastructure respondents have experienced a major impact due to a security compromise of an IoT device.**

Respondents in critical infrastructure organizations are aware of the severity of the risks they face. Most understand the consequences of a security breach, and they see the proliferation of mobile and IoT devices as a formidable security challenge. Nonetheless, rapid adoption continues.

87%

**of critical infrastructure respondents believe a security breach involving mobile and IoT devices would have a substantial impact on their business.**

86%

**of critical infrastructure respondents agree that security risks associated with mobile and IoT devices have escalated over the past year.**

44%

**of critical infrastructure respondents identify “integration of mobile and IoT services” as a daunting security challenge.**

## Top target: Energy and utilities

Critical infrastructure organizations see great benefit from the efficiencies and visibility that IoT brings. In the energy sector, sensors help workers detect transmission line and power station outages. Using data analytics, energy providers can better direct power across the grid to balance supply and demand, while helping to maximize the integration of renewable energy sources. Smart meters and thermostats are increasingly coming online in homes and businesses, providing data that utility companies now use to improve services.

It's no surprise IoT adoption is close to universal in the energy and utility sectors. But it's critical for these organizations to develop smart risk management strategies, since threat actors have increasingly demonstrated eagerness to target them. Look no further than the Colonial Pipeline ransomware attack, the Saudi Aramco drone strike, or the sabotage of the Nord Stream pipelines to appreciate the vast geopolitical consequences of such activities.

90%

**of energy and utilities respondents agree that managing the nation's critical infrastructure makes them a prime target for cybercriminals.**

## Another prime target: Public Sector

The Public Sector also faces significant mobile and IoT-related security risks. According to the 2024 Data Breach Investigations Report, Public Administration is a top target for organized crime, along with state-affiliated threat actors (together responsible for 96% of breaches caused by external actors in which the actor type was known, n=305).<sup>7</sup> Thirty percent of breaches in this sector (when known) were espionage motivated.<sup>8</sup>

70%

**of Public Sector respondents report that their organizations experienced a security incident involving a mobile or IoT device.**

<sup>7</sup> Verizon, Data Breach Investigations Report, 2024.

<sup>8</sup> Ibid.

# All sectors perceive increased mobile and IoT risk.

Since we launched this report seven years ago, we've seen the percentage of companies that suffered a mobile compromise trend steadily upward, from less than 30% in 2018 to more than half (53%) today. Some of this increase is related to the expanding attack surface. As mobile and IoT devices are embedded into all types of workflows, the sheer number of devices and apps that businesses rely on snowballs (as do the risks).

### Perceived mobile device security risk

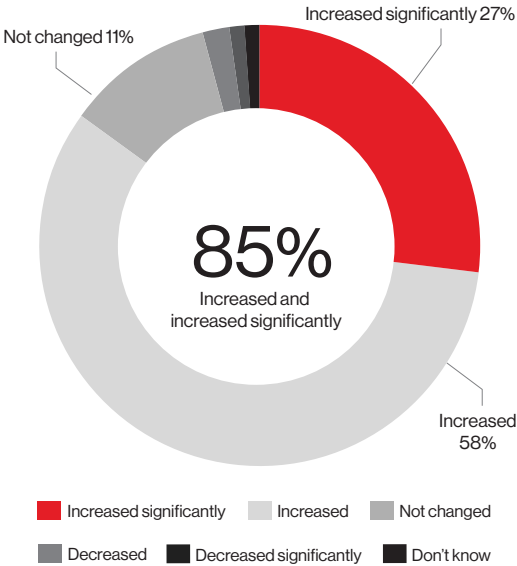


Figure 3: Among organizations allowing Wi-Fi and/or cellular access, some type of security is in place with SASE and VPN as most prevalent.

At the same time, alongside device numbers, awareness of mobile-specific security risks has also grown. Many people once thought that mobile devices were inherently more secure than desktop or laptop computers. Not anymore. A large majority of respondents (85%) now recognize that mobile device threats are on the rise, and more than half of those surveyed have experienced security incidents firsthand.

**85%**  
of respondents say risks from mobile device threats have increased in the past year.

**64%**  
believe they are at significant or extreme risk from mobile device threats.

**51%**  
have experienced mobile app-related incidents from factors such as malware or unpatched vulnerabilities.

## Awareness vs. real-world risks

For business users and consumers, 2023 was a record-breaking year for mobile threats. More zero-day vulnerabilities were discovered in iOS than ever before. The risky data collection policies used by popular apps such as TikTok and PinDuoDuo were on public display, while 75% of organizations experienced mobile phishing attempts targeting their employees.<sup>9</sup>

# 33%

of mobile phishing attacks against technology company employees in 2023 were successful.<sup>10</sup>

# 27%

of mobile phishing attacks against the financial sector succeeded.<sup>11</sup>

# 21%

of mobile phishing attacks targeting media and communications companies succeeded.<sup>12</sup>

## In 2023, almost every iOS update that users were asked to install on their smartphones involved a security vulnerability.<sup>13</sup>

More than 260 iOS Common Vulnerabilities and Exposures (CVEs) were published in 2023. Because so many mobile device operating systems aren't updated as often as they should be, the data and personal information stored on or accessible through them remain susceptible to exploits for extended periods of time. And the number of attacks that exploited vulnerabilities as the critical path to initiate a breach nearly tripled (a 180% increase) in 2023 compared to the prior year.<sup>14</sup> Some of this growth is due to enormously successful widespread campaigns, such as the CIOp ransomware gang's exploitation of the MOVEit file transfer tool, which ultimately impacted millions of victims.<sup>15</sup>



## Top Android vulnerabilities in 2023<sup>16</sup>

**CVE-2023-5217:** A vulnerability in a video codex library used by Chrome, Firefox and Firefox Focus for Android

**CVE-2023-6345:** A vulnerability in the 2D graphics engine for Google Chrome, Chrome OS, Android and Microsoft Edge

**CVE-2023-3019:** A zero-day vulnerability in the V8 JavaScript engine of Chromium impacting versions of Google Chrome and Microsoft Edge mobile browsers

**CVE-2023-2033\_2136:** A group of vulnerabilities, some impacting Samsung devices and others affecting all Android devices

**CVE-2023-4863:** A vulnerability in Chrome for Android's WebP image format. A similar image processing vulnerability, BlastPass, has been exploited to deliver spyware

9 Lookout, Mobile Threat Landscape Report, 2023.

10 Akamai, The Increased Use of Mobile Devices Expands the Threat Landscape, 2023.

11 Ibid.

12 Ibid.

13 Ibid.

14 Verizon, Data Breach Investigations Report, 2024.

15 Ibid.

16 Lookout, Mobile Threat Landscape Report, 2023.

# Mobile and IoT security lags behind usage.

Our ongoing reliance on mobile devices and rapid increase in IoT use generates opportunities for attackers to take advantage of key vulnerabilities, including as-yet-undiscovered zero-day attacks.

The vast majority of respondents (93%) express concern about mobile cybersecurity risks. Nonetheless, a minority (39%) have defined organizationwide IoT standards, and even fewer (37%) say their organizations centrally coordinate IoT projects.

Defining and adhering to cross-organizational standards is crucial to helping ensure IoT devices and sensors can keep up with evolving security and regulatory requirements. With enormous variability in device capabilities, use cases and risks, it's important to set technical and non-technical standards for each IoT project across every business unit.

87%

of respondents believe a security breach could severely impact the business's operations.

39%


have defined IoT standards.

37%

centrally coordinate IoT projects.

The National Institute of Standards and Technology (NIST) recommends baselining the following core technical capabilities:<sup>17</sup>

 Device identification

 Device configuration

 Data protection

 Logical access to interfaces

 Software updates

 Cybersecurity state awareness

NIST also recommends setting standards for non-technical aspects of IoT projects, including:<sup>18</sup>

 Documentation

 Responding to queries

 Information sharing

 Education and awareness

<sup>17</sup> NIST, NIST Cybersecurity for IoT Program, Create a Profile Using the IoT Core Baseline and Non-Technical Baseline, 2020.

<sup>18</sup> Ibid.



# Mobile phishing

Data is the currency of modern enterprises. Establishing a strong data security strategy is not only a critical defense measure, but also a strategic business enabler.

In years past, organizations had dedicated private data centers, housing multiple servers, network equipment and storage devices. These setups not only presented scalability issues, but required continuous hardware and software upgrades to accommodate rising data needs. If not well maintained, this infrastructure is also highly susceptible to malware and vulnerability-based attacks.

Today, a majority of corporate data resides in the cloud across an increasing number of software-as-a-service (SaaS) and private apps. While this infrastructure is better maintained, making network bugs less of a concern, critical corporate data is also more widely distributed. This distribution presents other challenges, such as the risk of system misconfigurations, as sensitive data flows across an expanding set of apps.

With more corporate data residing in the cloud, we're seeing a shift away from traditional malware and vulnerability attacks. Because cloud infrastructure is better maintained, the return on investment for traditional exploits has diminished. In response, threat actors have changed their Tactics, Techniques and Procedures (TTPs), to focus on leveraging social engineering, targeting a user's mobile phone to steal credentials and impersonate users. With credentials in hand, they have immediate access to critical corporate infrastructure and sensitive data. We refer to this change in TTP strategy as the modern kill chain.

To illustrate, consider recent high-profile attacks: MGM Resorts, Caesars Entertainment and Twilio. In each instance, the threat actor group known as Scattered Spider used the phishing kit Oktapus to social engineer via mobile devices. In another example, the Lookout Threat Intel team discovered a similar phishing kit, CryptoChameleon that has been used by what was likely a different group of threat actors to target the FCC, Coinbase, Google, Microsoft and other organizations.

If a phishing attack is successful and a threat actor is able to get login credentials, the subsequent steps in the modern kill chain move rapidly. With direct access to an organization's cloud infrastructure, the attack dwell time has gone from months to minutes. This also brings severe repercussions for individuals, who are at risk of identity theft, along with the organizations that are required to safeguard sensitive data. Defending against rapid modern attacks requires organizations to have clear visibility and automated response capabilities, both at the mobile endpoint and across their software as a service (SaaS) and private applications.



**Aaron Cockerill**  
Executive Vice President  
of Product & Security  
Lookout

# 25%

**of mobile users  
tapped on at least  
one phishing link  
every quarter in  
2023.<sup>19</sup>**

<sup>19</sup> Lookout, Mobile Threat Landscape Report, 2023.

# Breach risks and impacts are high, especially in critical infrastructure.

**Mobile security risks are real—and expanding. All types of organizations are adding mobile and IoT devices into their daily operational processes, without extending robust protections across all endpoints. As a result, the attack surface is expanding. Again, critical infrastructure is at heightened risk overall, from increased IoT use to legacy systems and equipment to nation-state targeting.**

## **Mobile incidents and consequences**

Not only are mobile compromises trending up, but the consequences of breach incidents can be profound. Widespread bring-your-own-device (BYOD) policies have led to corporate, sensitive or regulated data being stored on or passing through mobile devices. And because mobile devices are so easy to carry, they're also easy to steal. If a mobile device has high-value data stored on it, a breach can result in the immediate loss or theft of that data, especially if the device's lock screen is disabled or it doesn't have remote-deletion capabilities.

It's especially worrisome that attackers who compromise a mobile device frequently use the infected device to gain access to company networks. This can result in large-scale data exfiltration, the spread of ransomware, customer and employee privacy violations and costly operational downtime.

**53%**

**of respondents experienced an organizational security incident involving a mobile or IoT device that resulted in data loss or downtime.**

**25%**

**of organizations have at least one mobile device user on staff who has disabled their lock screen feature, even though only 3% of all devices have the lock screen disabled.<sup>20</sup>**

**47%**

**report that such compromises had major impacts on their organizations.**

<sup>20</sup> Jamf, Security 360: Annual Trends Report, 2024.

# The potentially high cost of breaches to critical infrastructure

Consequences of a mobile-related breach can be especially devastating for organizations in critical infrastructure sectors. Mobile—and especially IoT—devices are embedded in mission-critical processes and workflows. A breach or failure can disrupt operations and has the potential to impact human health and safety.

85%

of Public Sector respondents agree that a security breach of their organization could endanger lives, especially if critical or emergency services go down.

92%

of healthcare respondents agree that the highly confidential nature of patient data makes their organization a prime target for cybercriminals.

82%

of manufacturing respondents agree that a security compromise could disrupt their company's supply chain, bringing serious financial implications.



Critical infrastructure organizations tend to face higher remediation costs and downstream losses when a breach occurs. Among respondents in critical infrastructure organizations that had suffered a compromise:



Nearly half (40%) admit they experienced damage to their reputations and loss of business.



More than a quarter (28%) report that addressing the incident required expensive remediation.

# Mobile attack objectives and how to address them



**Michael Covington**

Vice President,  
Portfolio Strategy  
Jamf

According to research from Jamf, the majority of malicious actors targeting mobile devices are trying to achieve one of the six goals outlined below.<sup>21</sup> That's why it's a good idea to follow best practices adapted for mobile from standards such as the NIST Cybersecurity Framework and Center for Internet Security (CIS) Benchmarks to help protect your organization.



**Gain access to confidential business data.** Attackers are frequently motivated by financial gains or competitive advantages; theft of intellectual property is frequently cited as a top motivator for developing malware.



**Spy on users without their knowledge or consent.** Threat actors have been observed taking advantage of the always-on, always-with-us nature of mobile devices to listen to conversations, intercept SMS messages and track physical movements through GPS.



**Bypass internal security protections.** Modern operating systems like iOS have built-in protections to restrict what can run on mobile devices. Changes to Apple's controlled distribution model via regulation like the EU's Digital Markets Act is reducing the efficacy of those once controlled walls built to protect the mobile device.



**Obtain private data without authorization.** Researchers at Jamf have seen malicious apps circumventing Apple's Transparency, Consent and Controls (TCC) as part of the attack chain targeting Apple users, ultimately weakening built-in protections and making device compromise easier. Apple's mobile devices have similar features in place to protect end user privacy that can also be tampered with as the attacker looks for the weak links in the chain.



**Run malicious code on devices.** Zero-click exploits are well-documented, but vendors are quick to patch vulnerabilities that are exposed to the remote attacker. The ultimate goal is usually for the attacker to gain a foothold on the device from which they can surveil, exfiltrate data or pivot to another asset.



**Pivot from an infected device to compromise networks.** Beyond data theft, privacy compromises and persistence objectives, it's not uncommon for attackers to simply use a compromised (and trusted) mobile endpoint to move closer to the more valuable target within the organization.

21 Jamf, Security 360: Annual Trends Report, 2024.

# Shadow IT: A looming security challenge

**Whose mobile device is that? Where did it come from? How did it get connected to our network? Is its operating system up to date? Does it meet compliance requirements? These questions are being asked by security professionals inside many organizations today. And as mobile and IoT devices continually connect to enterprise networks, many organizations face challenges in keeping track of them all.**

## Out of the shadows

We define shadow IT as the use of hardware or software by a department or individual without the knowledge or oversight of the organization's IT or security team. Shadow IT adoption takes place across all sectors. With so many organizations prioritizing agility and end-user experiences and too few building universal security policies across locations and device types, there's fertile ground in many enterprises for shadow IT to grow, creating additional security risks.

Without oversight, shadow IT devices are at high risk of misconfiguration, having out-of-date or unpatched software such as apps and operating systems, or having insecure apps downloaded from an untrustworthy source. As a result, end-users are vulnerable to phishing, malware and other attacks.

Survey respondents indicate growing concerns about the risks unmanaged devices pose.

**54%**

**are very or quite worried about shadow IT.**

**87%**

**of respondents are at least somewhat worried about shadow IT.**

## BYOD risks

Companies that allowed employees to use their own devices at work peaked in 2021, in the aftermath of the COVID-19 pandemic.<sup>22</sup> Since then, BYOD adoption has stabilized, with a majority of companies either allowing or considering allowing personal device use for work-related tasks.

Securing employee-owned devices is often considerably more difficult than securing corporate devices, especially without a mobile device management (MDM) solution in place. In reality, adopting a BYOD policy means making a concession: It's the same as saying that some shadow IT is okay. If employees are allowed to use their personal devices at work, everyone in the organization is entrusted with responsibilities that once belonged only to the IT department. Still, many organizations offer BYOD policies.

**59%**

**of respondents allow employees to access work email from their personal phones/devices.**

**An additional 34%**

**are considering doing so.**

## Secure connectivity

It's not just mobile device vulnerabilities that generate risks. Insecure connectivity makes it easier to steal data or compromise the confidentiality of sensitive information. For many organizations, the pressure's on to allow remote workers to use public Wi-Fi, home Wi-Fi and cellular networks. Even those that don't explicitly allow these types of connectivity often struggle to prevent it in real-world scenarios.

37%

of employees in organizations that ban (or don't have a policy on) the use of public Wi-Fi use it anyway.

45%

of employees in organizations that ban (or don't have a policy on) the use of home Wi-Fi use it anyway.

26%

of employees in organizations that ban (or don't have a policy on) the use of cellular networks or hotspots use them anyway.

## Security tools and policy advantages

Research from Ivanti shows that today's top employees prefer workplace policies that include flexible scheduling and hybrid work that allow them to work where and when they're most productive.<sup>23</sup>

80%

of office-based workers highly value workplace flexibility, or find it something they can't do without.<sup>24</sup>

41%

would consider changing jobs to gain more flexibility at work.<sup>25</sup>

79%

agree letting people work anywhere is the future of professional employment.<sup>26</sup>

<sup>23</sup> Ivanti, Everywhere Work Report, 2024.

<sup>24</sup> Ibid.

<sup>25</sup> Ibid.

<sup>26</sup> Ibid.

To meet their employees' rising expectations, companies provide support and solutions to enable them to work securely, regardless of their location. Organizations that have defined policies for allowing public or home Wi-Fi use or the use of cellular networks for work purposes have an edge here.

**Nearly all respondents (99+%) indicate their organizations have implemented remote access security technologies. The most commonly used solutions in this category include:**



**Virtual private networks (VPNs)**



**Cloud access security broker (CASB) tools**



**Identity and access management (IAM) platforms**



**Multi-factor authentication (MFA)**

### Wi-Fi / cellular security

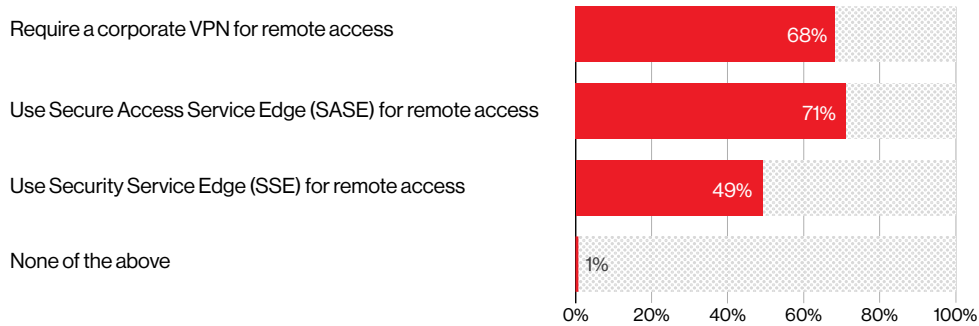


Figure 4: Among organizations allowing Wi-Fi and/or cellular access, some type of security is in place with SASE and VPN as most prevalent.

**In addition, more than two-thirds (66%) of respondents now apply centralized security standards across all projects involving mobile devices and more than half (58%) of IT departments have oversight across these projects.**



# Emerging AI cyberthreats meet new AI defenses.

If there's one constant that's held steady throughout decades of cybercriminal activity, it's that threats are always evolving. Threat actors are the ultimate shape-shifters, forever changing their tactics as defenders adopt measures to counter them. What's different today is the accelerated pace of the evolution. The latest advances will allow attackers to launch more attacks faster than ever before.

## The generative AI revolution

Generative AI tools like ChatGPT and Google Gemini have been making headlines and dominating conversations for the last year. At the moment, we may be in a grace period when it comes to mobile security and AI-enabled cyberattacks. According to the 2024 Verizon Data Breach Investigations Report, there's not much evidence cybercriminals are yet harnessing these tools to carry out attacks at scale.<sup>27</sup>

However, it's likely that threat actors are experimenting with generative AI now, building their skills and bots that will eventually let them use Gen AI to code malware more quickly, or scale up the volume of highly effective and targeted phishing attacks.

## AI threats yet to come

Expanding AI use will likely lead to an increase in the volume of attacks criminals launch within the next year. It's also possible that more frequent attacks will have a greater impact. Initial changes to the threat landscape are likely to be subtle – until they're not. As is typical in the dynamic world of cybersecurity, a widespread new exploit can change the picture overnight.

Threat actors of all types, from the most sophisticated nation-states and highly resourced criminal syndicates to solo cybercriminals, will eventually adopt AI. They'll go for the least sophisticated, lowest-effort applications first. Generating more phishing messages? Pretty simple. Translating social engineering attempts into multiple languages? Done.

With AI threats on the horizon, defenders should prepare now for the next generation of attacks. And they should be on the lookout for AI-assisted attacks involving deepfakes and SMS phishing, which will likely form the first wave of AI-powered threats.<sup>28</sup>

**As AI-driven cyberthreats loom, defenders, including cybersecurity vendors such as Verizon, are working quickly to incorporate AI technology into mobile security tools and services. These solutions can help and are already helping organizations gain faster, better, more in-depth threat monitoring, access verification, and real-time phishing detection.**

77%

**of respondents believe AI-assisted attacks like deepfakes and SMS phishing are likely to succeed.**

88%

**believe that AI-assisted cybersecurity solutions will become increasingly important in the future.**

<sup>27</sup> Verizon, Data Breach Investigations Report, 2024.

<sup>28</sup> Ibid.

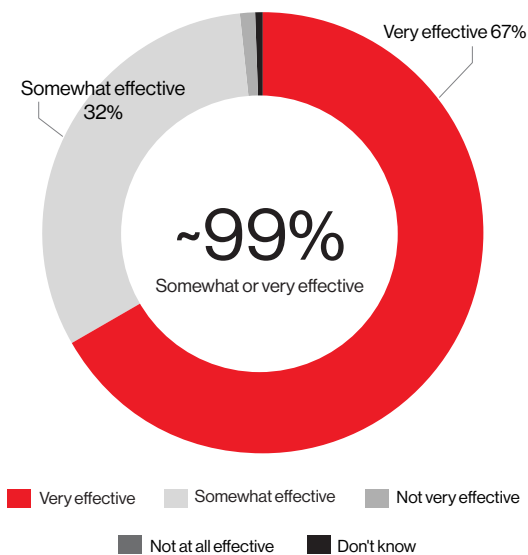
# The disconnect between perceived and actual mobile security

Despite rising concerns about everything from breach risks to mobile-driven attacks and potential AI threats, survey data leads us to believe that the extent of concern shown by respondents often doesn't seem to match the risks.

## A false sense of security

Respondents report high levels of confidence in their mobile defenses across a number of areas. For instance, they express a great deal of faith that current mobile device security measures are effective, with 96% asserting that their defenses are at least somewhat effective.

How would you rate the effectiveness of your organization's mobile device security measures?



**This confidence stands in stark contrast to rising reported breach rates.**

67%

say current mobile device security measures were very effective.

53%

have experienced a security incident involving a mobile or IoT device that resulted in data loss or downtime.

Figure 5: Nearly 99% of respondents rate their organization's mobile device security measures as somewhat to very effective. Figures are rounded to the nearest whole number.

## Compromised? No problem.

Another area where respondents express high levels of confidence was in their ability to recover quickly from a breach incident.

**If your company were compromised, how confident are you that you would be able to recover quickly?**

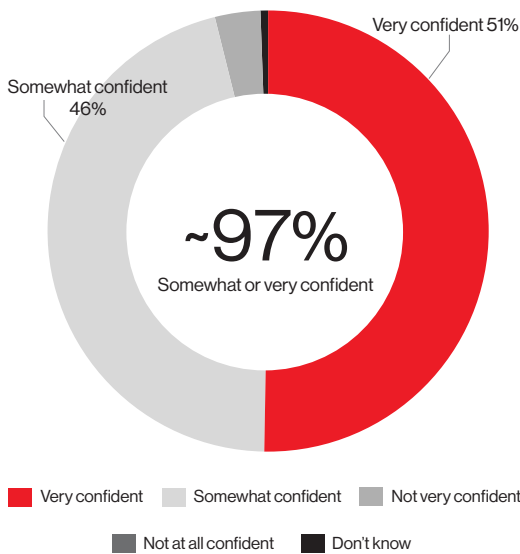


Figure 6: Nearly 97% of respondents are somewhat to very confident in their ability to rapidly recover from a breach. Figures are rounded to the nearest whole number.

**This, too, is at odds with what respondents say about their actual incident experiences.**

**51%**

**are very confident in their ability to quickly recover from a mobile-related compromise.**

**38%**

**report that an organizational security incident involving a mobile or IoT device had a major impact—financial or reputational—on their organization.**

**75%**

**of those that experienced a mobile- or IoT-related incident say remediation was not simple or cheap.**

## Underlying unease

Despite a professed confidence in their ability to protect against mobile-based threats and recover from incidents, respondents also simultaneously cite persistent mobile security worries. Almost half believe end users are complacent about data privacy and security, oblivious to the dangers of credential theft, and tend to exercise poor security hygiene.

## Lack of visibility and control

Part of the problem could be that respondents simply don't know what they don't know. With the proliferation of shadow IT, little centralized IT oversight of IoT projects and many employees taking a choose-your-own-adventure approach to home and public Wi-Fi connectivity, security stakeholders face a daunting challenge in accurately assessing the risks.

87%

say they are at least somewhat worried about shadow IT.

89%

of respondents believe organizations need to take mobile device security more seriously.

63%

of respondents do not centrally coordinate IoT projects.

55%

have no formal disaster recovery plan in place.

85%

of respondents believe mobile-related security risks have increased or significantly increased over the past year.

53%

report that IT does not have oversight of IoT projects.

41%

lack organizationwide security policies.

# Critical infrastructure sectors have specific considerations.

Mobile and IoT-related risks are a reality across industries, but every vertical is unique. Each has its own threat profile, its own use cases for IoT deployments and its own regulatory requirements.

While mobile security challenges exist across all industries, these risks were found to be elevated across critical infrastructure sectors.

## Energy

The energy sector has long been a top target of nation-state attackers interested in disrupting operations, stealing information assets and harming the economy, according to the International Energy Forum.

What's more, energy sector companies are caught between a rock and a hard place when it comes to IoT implementation. These devices are viewed as essential to optimizing processes by most respondents (64%), but nearly as many (62%) view IoT as a major security challenge.

Nearly half of respondents (49%) view greater use of IoT-enabled services as vital to improving employee safety. Of course, a major breach involving cyber-physical systems in this industry has the potential to threaten human health and safety, too. How's that for a paradox?

90%

of energy sector respondents agree that managing the nation's infrastructure makes them a target for cybercriminals.

### Energy Sector

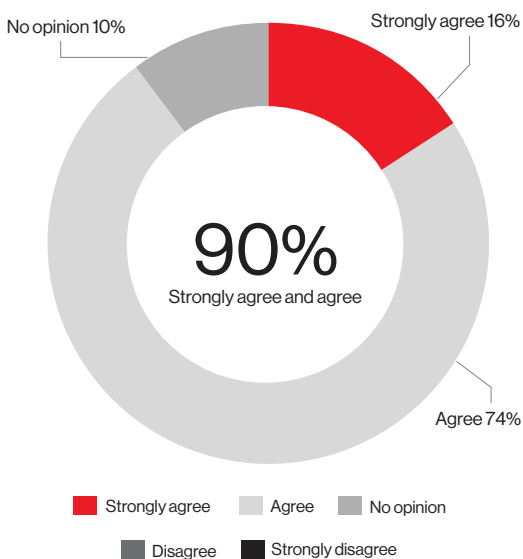


Figure 7: 90% of energy sector respondents agree or strongly agree that managing the nation's critical infrastructure makes them a prime target for cybercriminals.

# Public Sector

The Public Sector’s mission—to provide the essential services necessary for public welfare—makes it an attractive target for malicious actors looking for ways to cause far-reaching societal harm. At the same time, accelerating digital transformation of public services can make it faster, easier and more efficient for government organizations to meet the needs of their constituents. Mainly taxpayer-funded, Public Sector entities must also operate within firm budgetary constraints, making the efficiencies delivered by IoT particularly attractive.

The desire to digitize services for greater efficiency and cost benefit is driving significant IoT adoption in the Public Sector. Public Sector respondents to our survey agree that increased use of IoT is essential for accelerating their digital transformation and meeting budget pressures. However, nearly half (47%) cite IoT use as a daunting security and privacy challenge as well. Yet a majority prioritizes cost-efficient digital service delivery over cybersecurity risk.

Unfortunately, the risks are severe. A significant majority (85%) of Public Sector respondents believe that a security breach in their industry could endanger human lives.

## Public Sector

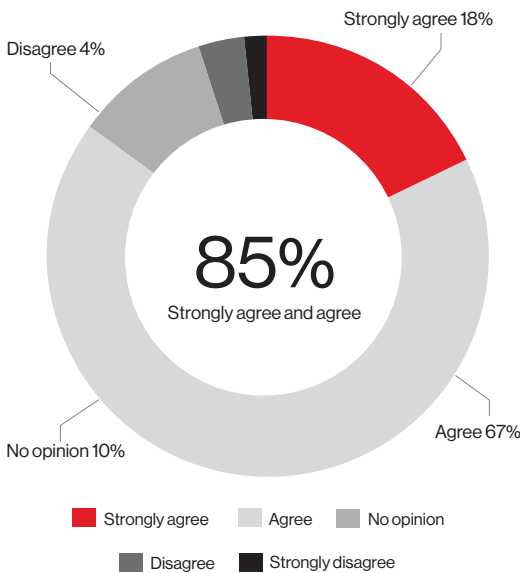


Figure 8: 85% of Public Sector respondents agree or strongly agree that a security breach could put people’s lives at risk (e.g., if critical or emergency services went down).

# Healthcare

Along with digital healthcare technology, the Internet of Medical Things (IoMT) is poised to transform every aspect of patient care from appointment scheduling to diagnostics, all the way through to continuous glucose, temperature and cardiac monitoring—and beyond.

The potential consequences of a security breach in this sector are also severe, especially considering what could happen if connected medical devices are targeted, given the role they play in critical care and life-support systems.

Telehealth is perceived as presenting a valuable opportunity to improve patient care and an opportunity for growth by more than two-thirds of healthcare sector respondents (71% and 67%, respectively). Less than half (44%) understand telehealth adoption as a daunting security and privacy challenge. For many stakeholders in this sector, improving the quality of patient care is a higher priority than mitigating cyber risk. At the same time, more than nine in 10 respondents (92%) believe that their industry is a top target for cybercriminals.

**92%**  
**of healthcare respondents agree that the confidential nature of patient data makes their industry a target for cybercriminals.**

## Healthcare

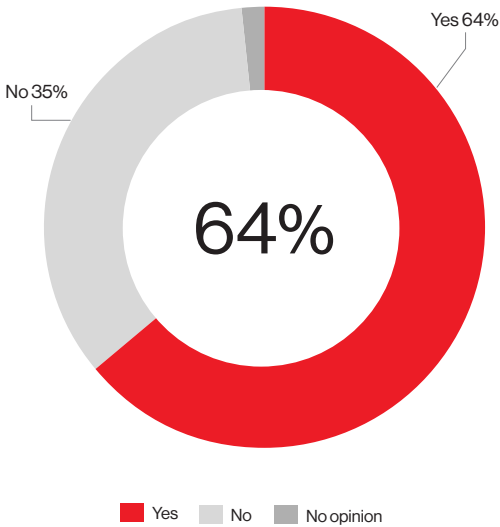


Figure 9: 64% of healthcare respondents' organizations allow remote access to electronic patient records.

## Financial services

Since the start of the pandemic, mobile banking has rapidly evolved from a “nice to have” to a “can’t live without” for many consumers. To meet customer expectations, financial institutions must deliver convenient, friction-free digital experiences to their customers—at any time, in any place, on any device. At the same time, criminals tend to go where the money is, making banks and financial services firms a high-value target. Balancing regulatory constraints, attractiveness to bad actors and the convenience needs of customers is no easy task.

Financial sector respondents believe that using mobile-based services is essential if they are to stay relevant to consumers, but they also think that maintaining a strong cybersecurity reputation is vital for attracting and retaining their customers.

**85%**

**of financial sector respondents agree that using mobile-based services is essential for being innovative and staying relevant to consumers.**

**68%**

**agree that having a good cybersecurity reputation is important for retaining existing customers.**

**70%**

**agree that using mobile-based services increases their agility and responsiveness.**

**66%**

**agree that having a good cybersecurity reputation helps them attract new customers.**



# Manufacturing

In manufacturing, efficiency and productivity are major drivers of revenue growth. It follows that IoT adoption by manufacturing organizations can offer enormous benefits. Embedding sensors into production processes can optimize throughput, enable predictive maintenance analytics to prevent downtime and improve quality control. IoT devices can also gather the data that manufacturers need to meet environmental, social and governance (ESG) objectives.

With all of these potential benefits, it's no surprise that the use of IoT devices and mobile-based services is on the rise among manufacturing sector respondents. What's concerning, however, is that increasing operational technology (OT) and IT convergence – and with it the added connectivity between networks and physical production operations – both raise the possibility that a breach could jeopardize expensive infrastructure, as well as human health and safety. When digital devices control physical systems like robotic arms, cyber risks potentially become risks to life and limb.

## Manufacturing: Increasing mobile services use on the shop floor

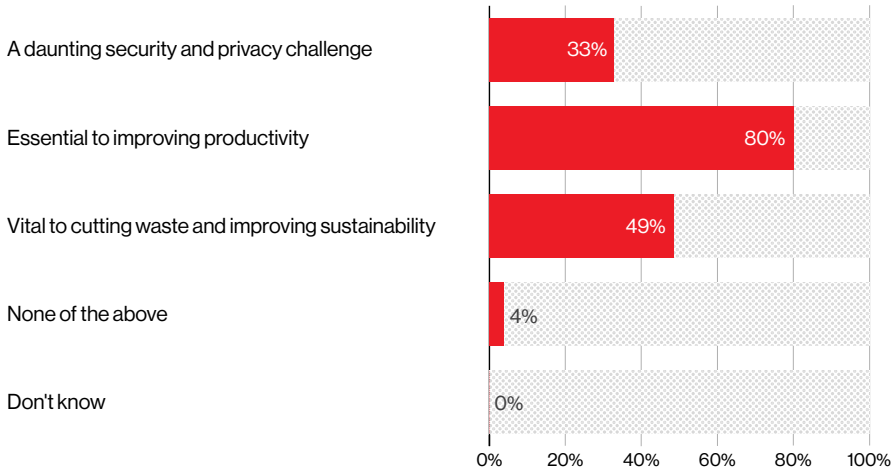


Figure 10

**90%**  
of manufacturing respondents agree that growing OT and IT integration makes mobile device security more critical.

**92%**  
of manufacturers are using IoT devices.

# Mobile security awareness and solution investments are rising.

While the survey illuminates some worrisome trends, there's also good news to share.

As large-scale ransomware attacks and data breaches now regularly make headlines, stakeholders have taken notice. Mobile security spending has been on the rise for years, and the pace is likely to increase as greater awareness of the risks and costs of breaches drives organizations to centralize controls, standardize security policies and deploy effective solutions.

## Security spending is up.

Investments in securing mobile and IoT devices are rising. In fact, more than four in five organizations (84%) increased mobile device security spending over the past year. The increases were driven by a rising volume and greater awareness of threats, along with increased remote work. And spending is likely to increase in next year's budget too, which is an encouraging sign that more organizations are taking a harder look at mobile security.

84%

of respondents increased or significantly increased mobile security spending in the past year.

86%

anticipate further increasing mobile security spending next year.

### Drivers of increased mobile security spend

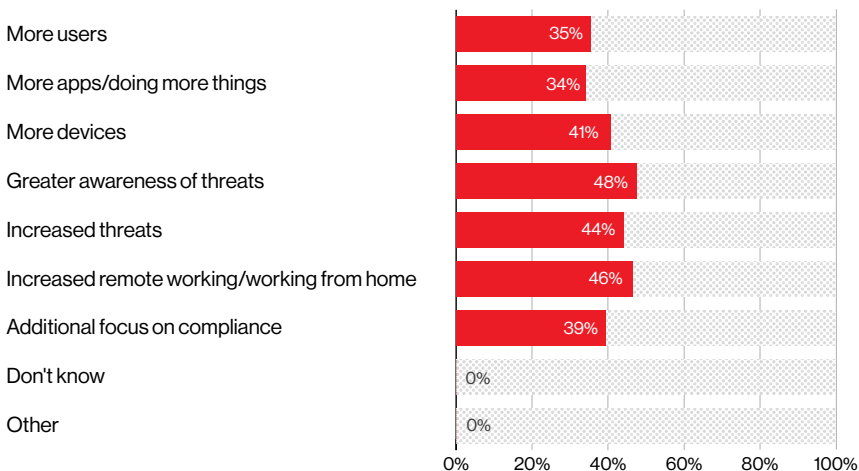


Figure 11

# Critical infrastructure steps up.

Also good news: Critical infrastructure organizations are increasing their spending to match or exceed other sectors. 84% of those surveyed said mobile security spending has grown in the past year. And they're even more likely to be planning to invest more in the year ahead. Because the growing importance of AI to cyber defense is widely recognized, a number of these investments will likely be in AI-powered solutions.

# Covering the bases

The NIST Cybersecurity Framework (NIST CSF) originally covered five key functions of a healthy cybersecurity program: Identify, Protect, Detect, Respond and Recover. In February 2024, NIST added an additional function, Govern. Together, these categories provide recommended steps and best practices across the cybersecurity function.

The Govern function covers risk management strategy, expectations and policy. It designates roles and responsibilities to foster stakeholder accountability. It also addresses cybersecurity supply chain risk management.

Perhaps because this function was so recently introduced, it's seeing a slightly lower level of investment. Otherwise, spending is expanding across all functions, with investments balanced across each area of protection.

**89%**  
of critical infrastructure respondents plan to increase or significantly increase mobile security spending in the next year.

**88%**  
recognize the increasing importance of AI-assisted cybersecurity solutions.

Security spend on NIST CSF categories: 2022 vs. 2024

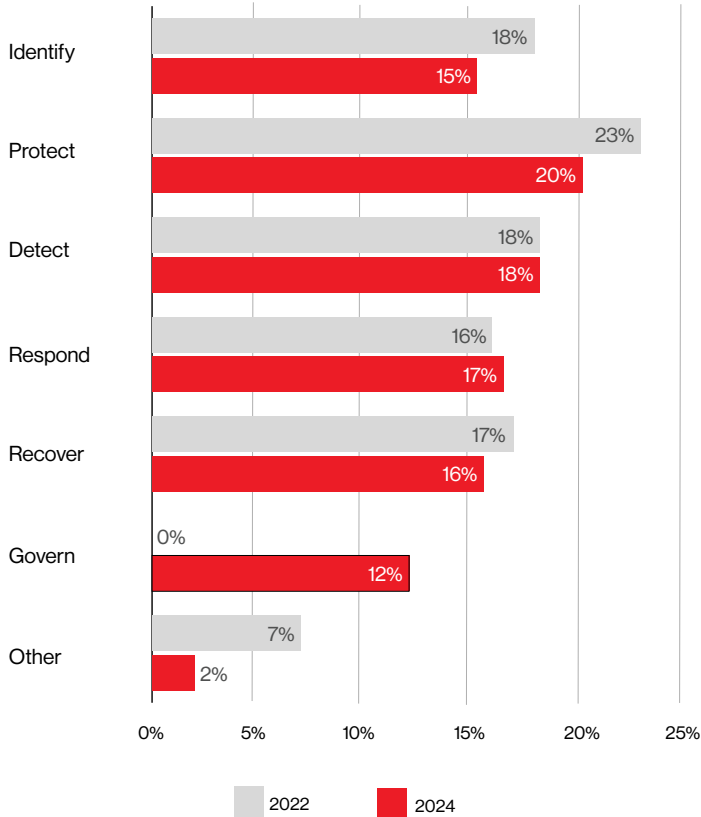


Figure 12

# The importance of an integrated approach to securing mobile networks

Only a platform-based approach to cybersecurity can manage the technological and architectural complexity associated with mobile connectivity to deliver effective and efficient protection and support compliance. Unlike point solutions, a cybersecurity platform integrates vendor-specific and third-party capabilities, allowing for greater automation, visibility and collaboration across endpoints, networks, clouds, applications and services. A mature cybersecurity platform will reduce operational costs, drive operational efficiencies and optimization, improve the organization's security posture overall and help maintain business continuity.

A platform approach offers several benefits, beginning with consolidated coverage that ensures organizations have fewer cybersecurity vendors to manage. It also features natively integrated capabilities that share information such as events, threats and telemetry from different parts of the network. This enhances visibility and control. By adding a high degree of automation, such a platform will be able to help reduce human error, accelerate threat response, improve outcomes and free staff to work on higher-value tasks.



## Above all, an integrated cybersecurity platform should:

---

Enable protection, detection and response to threats and vulnerabilities

---

Protect network exposure so that the enterprise can reliably deliver revenue-generating services and earn customer trust

---

Support compliance requirements, including those of customers

---

Make all of the above possible with automation and security operations (SecOps) capabilities

# IoT security is also making strides.

**More good news: Greater awareness is driving more investment in IoT security. And the expanding use of IoT security best practices, such as deploying organizationwide standards, centralizing coordination of IoT projects and devices, and applying more oversight for IoT projects, are also impacting IoT security spending.**

## **Keeping a close eye on “things”**

Among survey respondents who have deployed IoT devices, nearly all have applied at least some IoT security practices, and most are monitoring the effectiveness of encryption measures applied within IoT frameworks. Nearly four in five (79%) use automated tools for this purpose, while just under one-half (46%) are still relying on manual audits or third-party assessments.

**93%**

**of IoT users have applied at least some IoT security best practices.**

**70%**

**of IoT users have applied role-based access control to provision access to their devices.**

**96%**

**use automated solutions to monitor the effectiveness of the encryption measures used to protect IoT device data.**

The majority of respondents (69%) now have systems in place to track and automatically apply security patches to all of the IoT devices in their organizations. We can take this as a positive, in that modern IoT security practices are happening fairly widely. But it's also a negative result given how cyberattacks work. Cyberattacks are like water; threat actors find “leaks,” or gaps in coverage, and exploit them to launch an attack. The 31% of respondents citing no systems in place to automatically track and patch all IoT devices are shouldering substantial risk.

# But IoT security gaps remain.

**Even when organizations have IoT protections in place most of the time, or for most IoT sensors or devices, leaving any gaps open is all it takes to get through. And once inside, threat actors can move laterally, especially if network segmentation is lacking.**

**Organizations must be proactive and avoid complacency, especially in critical infrastructure sectors.**

## Mind the gaps.

In the 2022 MSI, 53% of responding organizations had defined IoT security standards that applied to all projects, and 48% of organizations centrally coordinated all of their IoT projects.<sup>29</sup> This year, only 39% of respondents say they have defined IoT security standards that apply to all projects, and just 47% have centralized coordination of all IoT projects.

These decreases are likely due to the extremely rapid pace of IoT adoption. When you're moving fast, it can be difficult for security to keep pace. The decrease may also be evidence of shadow IT projects, where individual lines of business coordinate their own projects without full, centralized control. No matter how you slice it, significant security policy gaps remain that translate to a higher degree of cyber risk.

**31%**

**of respondents do not have systems in place to track all IoT devices in their organizations.**

**46%**

**still rely on manual audits to keep track of IoT device encryption.**

**53%**

**lack centralized oversight of all IoT projects.**



<sup>29</sup> Verizon, Mobile Security Index, 2022.

# Secure the edge: how to safeguard your organization now



**Mike Riemer**  
Field Chief Information  
Security Officer  
Ivanti

## The edge under attack

Your edge devices are showing. And threat actors love it. In the era of Everywhere Work, edge devices are everywhere—and have become an attractive target for sophisticated attackers. These devices serve as entry points to an organization's network, allowing threat actors to move laterally and embed themselves. This can lead to significant data breaches and operational disruptions.

### Act now, defend your edge.

As the number of connected devices grows, securing edge devices becomes a necessity—not an option. Implementing proactive measures can significantly reduce an organization's attack surface, mitigate risks and maintain a robust security posture even when (and it's when, not if) threats morph, evolve and get smarter.

Don't allow edge devices to become the weak link in your network security chain. Take action now to protect your organization's valuable assets.

## Protect your edge, secure your network.

To combat the onslaught of threats, organizations must prioritize the following:

- 1. Timely patches:** Apply security patches to edge devices promptly when they become available.
- 2. Software updates:** Run the latest version of the solution's software on edge devices.
- 3. Continuous monitoring:** Monitor networks, including edge devices, for suspicious traffic and anomalies.
- 4. Zero trust:** Grant access only when necessary and verified, following zero trust principles.
- 5. Least privilege:** Give administrators and users only the permissions required for their roles.
- 6. Layered defense:** Use a multi-layered security approach, including firewalls, intrusion detection and endpoint protection.

# More to do. More that can be done.

Going forward, organizations need to take mobile security more seriously. The targeting of critical infrastructure, expanding use of IoT, emerging AI threats and other security drivers are relentlessly hammering organizations and spurring a new reckoning between executive leaders and security teams.

Another driver behind the need for improved mobile security is 5G, which is here and expanding rapidly. 5G networks are faster and more capable than ever before, encouraging people to use their mobile devices—and cellular data—for more tasks, more often. Within organizations of all types, this is likely to accelerate mobile and IoT deployment, ushering in a wide array of new uses and further enlarging the cybersecurity attack surface.

68%

of Verizon customers have 5G capable cell phones, up from 24% one year ago.<sup>30</sup>

56%

of data traffic runs over 4G services, compared with 81% one year ago.<sup>31</sup>

## Set security goals.

The designed-in security capabilities of 5G services are superior to those of 2G, 3G and 4G networks, with advances such as mutual authentication, improved subscriber identity protection and an inter-network security gateway. Still, 5G networks are open, and additional controls and protections must be implemented to protect mobile and IoT devices in enterprise environments.

Setting purposeful objectives is essential, but those goals may be even more critical for mobile security, where accelerated IoT growth, for example, is outpacing security coverage in most organizations.

Respondents are investing in mobile security to achieve the following objectives:

59%

are increasing the security of end user activities.

47%

are reducing the burden on IT (for instance, by automating tasks).

56%

are integrating security management of phones, tablets and laptops.

45%

are reducing inconvenience to users and increasing productivity.

48%

are enabling new services for remote workers.

<sup>30</sup> Verizon News Center, Massive, multi-year transformation of Verizon's network yields major benefits for customers, 2023.

<sup>31</sup> Ibid.



## Using industry standard frameworks

The vast majority of respondents (84%) have adopted or are considering adopting a cybersecurity framework. This move helps ensure that all departments and stakeholders are on the same page when it comes to adhering to industrywide best practices and standards. Approximately half (49%) of organizations are already using a secure service edge (SSE) framework, while 50% are using a secure access service edge (SASE) framework. More than two in five (44%) are currently considering SSE, with a slightly smaller percentage (42%) considering SASE. Both of these frameworks are converged approaches that bring cloud-native security technologies together into an integrated architecture to eliminate holes in protection and improve any organization's security posture.

Zero trust and the NIST CSF 2.0 are not yet widely adopted, but many organizations (45% and 48%, respectively) are considering each of them. However, a noteworthy minority of respondents say they've rejected or haven't given thought to the frameworks (16% for zero trust, 14% for the NIST CSF 2.0), revealing a trove of best practices and informational support that are not being taken advantage of.

# 83%

**of global organizations are planning to implement a converged security solution extending comprehensive security measures across services, networks and platforms.<sup>32</sup>**

### Security framework adoption

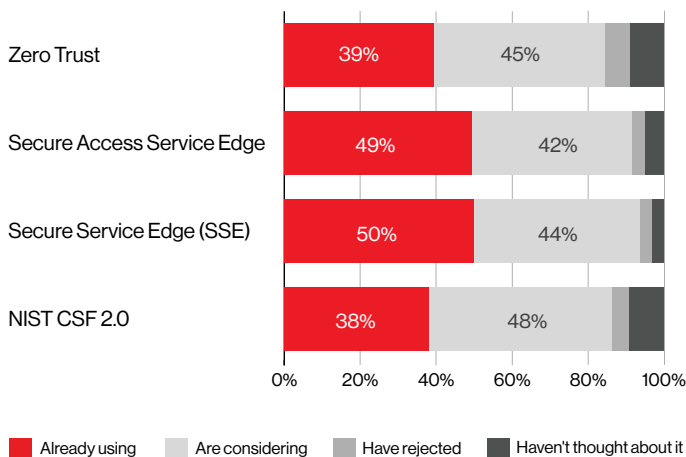


Figure 13

<sup>32</sup> Allot, Convergence Survey, 2023.

# The impact of compliance requirements

Regulatory requirements are another driver of mobile security investments. The two regulations to which the largest number of respondents are subject are the Department of Defense-aligned Cybersecurity Maturing Model Certification (CMMC) and Europe's General Data Protection Regulation (GDPR).

With CMMC 2.0 set to become a Final Rule in early 2025, a large number of defense contractors and subcontractors will need to improve their processes and controls to become audit-ready in the near future. At the same time, fines imposed for GDPR violations continue to rise, with approximately €2.1 billion in fines imposed in 2023 alone, which is more than all GDPR fines imposed in 2019, 2020 and 2021 combined.<sup>33</sup>

Another European framework, NIS2, will require critical infrastructure organizations to demonstrate specific cybersecurity protections and capabilities in the months and years ahead. The growing awareness of common risks and threats to critical infrastructure organizations, as well as government mandates to achieve an effective baseline of protection, can help accelerate cybersecurity best practices worldwide and lead to better defenses that combat rising threats to global citizenry.

In the not-too-distant future, the Securities and Exchange Commission's material incident disclosure requirement will likely have a significant impact as well.<sup>34</sup>

## Applicable compliance requirements

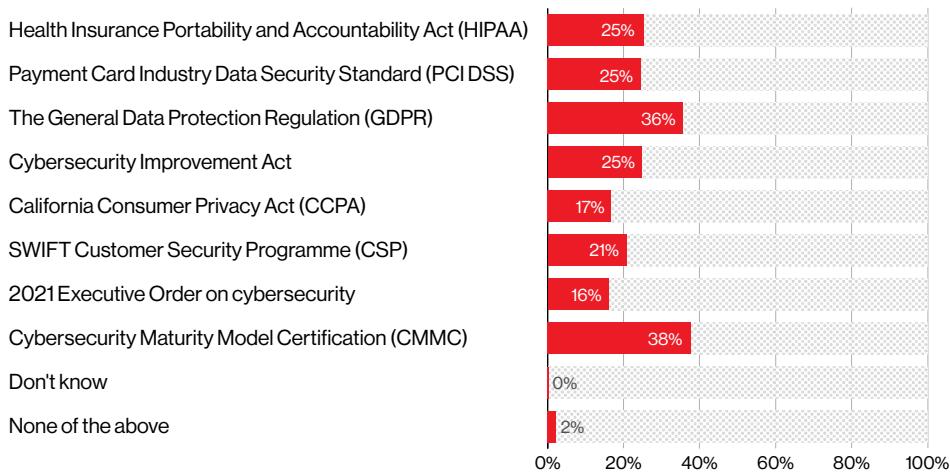


Figure 14

**As companies expand mobile and IoT connectivity, they'll need to embrace security standards that empower them to reap technological benefits without opening their organizations to security vulnerabilities that threaten operations and potentially even their livelihoods.**

**89%**

**of respondents agree organizations need to take mobile device security more seriously.**

<sup>33</sup> CMS, GDPR Enforcement Tracker Report, 2024.

<sup>34</sup> U.S. Securities and Exchange Commission, Statement: Cybersecurity Disclosure, 2023.

# The call to arms: Move faster.

**In putting together this report, we experienced moments of optimism as well as pessimism. While we were relieved to see positive indicators, like rising investments and awareness of mobile security and the growing adoption of technologies such as SASE to improve remote access security, organizational efforts are still falling short of recommended benchmarks.**

In a world where attacks can have devastating impacts on everything from production operations to revenue to reputation and even to people's health and safety, awareness is simply not enough. Unknown, unmanaged and unmonitored mobile and IoT devices can pose substantial security risks.

## **Critical infrastructure requires doubling down.**

Those responsible for securing the critical infrastructure that delivers our food, water, power, transportation, healthcare, emergency services and much more simply cannot take half measures. The potential consequences of a breach at a nuclear power plant or a regional hospital, for example, are simply too grave to ignore.

If people are to trust public services and consumers are to trust companies, organizational and security leaders must do more. They must strive for full visibility into all IoT projects across their organizations. They must enforce consistent standards for mobile security as well as IoT built-in device security, network segmentation and data encryption—everywhere.

They need to teach employees and end users about the dangers of credential theft, the importance of basic security hygiene, and the power of skepticism and situational awareness on an ongoing basis. And they should work tirelessly to build and cultivate a robust cybersecurity culture in their organizations. Anything less than unrelenting protection efforts is too little when the stakes are so high.

And it's not just about critical infrastructure organizations. Across all industry responses to our survey, similar patterns of mobile and IoT security gaps were present. That means there's work to do across the board. Public and private organizations must work together to deploy shield after shield, defense after defense, obstacle after obstacle, to foil threat actors attempting to interfere with the immense progress mobile and IoT connectivity delivers.

# 38%

**of critical infrastructure respondents know someone who has had a mobile device or mobile app hacked, compared to 36% of respondents in other industries.**

# 73%

**in critical infrastructure say leadership only takes cybersecurity seriously after a breach.**

## **Learn more.**

Help protect your business and learn more about mobile security risks at [verizon.com/mobilesecurityindex](https://www.verizon.com/mobilesecurityindex).

Or speak with your Verizon Account Representative.

# Appendices

# Survey methodology

We contracted with an independent research company to survey senior professionals responsible for the procurement, management and security of mobile devices.

In total, 600 professionals responsible for buying, managing and securing mobile devices took part in our survey. The charts below break down the demographics of respondents. Our sampled organization sizes included small companies through large enterprises.

**Regional location**

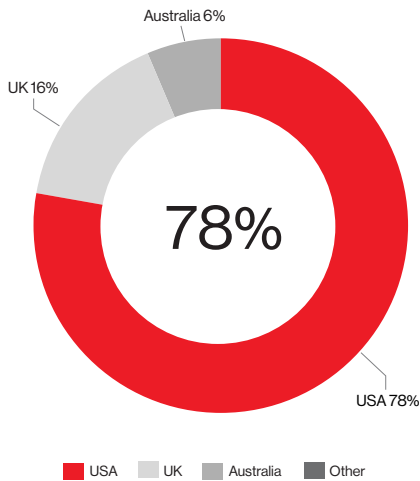


Figure 15

**Scope of operations**

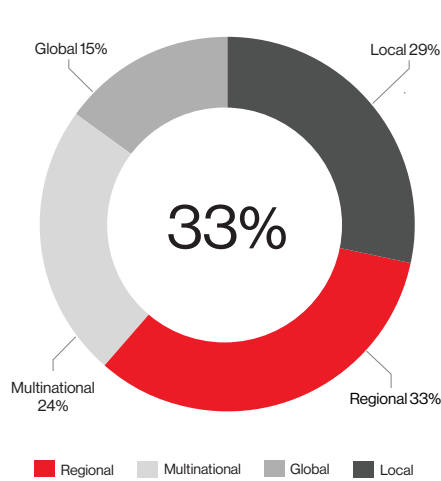


Figure 16

**Role function**

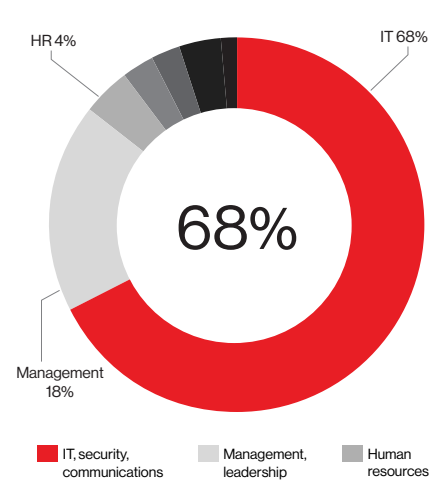


Figure 17

Respondents were distributed across 10 different vertical sectors, including six critical infrastructure sectors.

**Industry sectors represented**

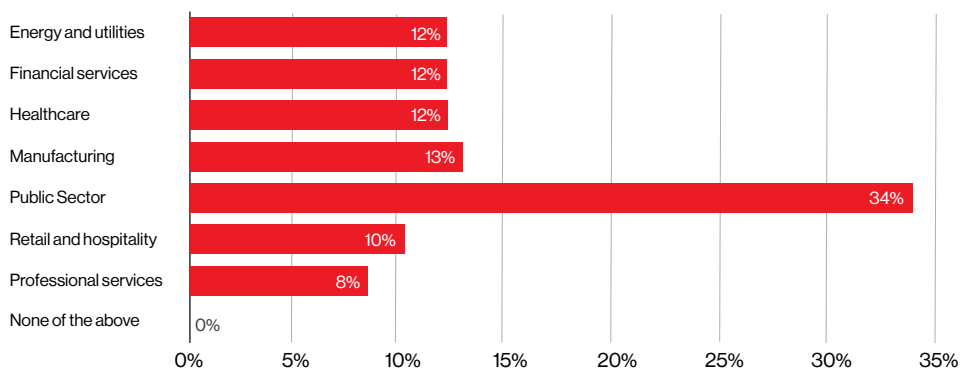


Figure 18

# Contributors



Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver and secure their digital experiences—helping billions of people live, work and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. For more information, please visit [akamai.com](https://akamai.com).



Allot is a leading provider of innovative network intelligence and security solutions that empower communications service providers (CSPs) and enterprises worldwide to enhance the value they bring to their customers. With over 20 years of proven success, our solutions turn network, application, usage and security data into actionable intelligence that make our customers' networks smarter and their users more secure. For more information, please visit [allot.com](https://allot.com).



Cisco (NASDAQ: CSCO) is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure and meet their sustainability goals. For more information, please visit [cisco.com](https://cisco.com).



Fortinet is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices and data everywhere. Today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Over half a million customers trust Fortinet's solutions, which are among the most deployed, patented and validated in the industry. The Fortinet Training Institute, one of the broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. Collaboration with high-profile, well-respected organizations from the public and private sectors, including CERTs, government entities and academia, is a fundamental aspect of Fortinet's commitment to enhance cyber resilience globally. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and top-rated protection and actionable threat intelligence. For more information, please visit [fortinet.com](https://fortinet.com).



Ivanti breaks down barriers between IT and security so that #EverywhereWork can thrive. Ivanti has created the first purpose-built technology platform for CIOs and CISOs—giving IT and security teams comprehensive software solutions that scale with their organizations' needs to enable, secure and elevate employees' experiences. The Ivanti platform is powered by Ivanti Neurons—a cloud-scale, intelligent hyper automation layer that enables proactive healing, user-friendly security across the organization and provides an employee experience that delights users.

Over 40,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com).



Jamf's purpose is to simplify work by helping organizations manage and secure an experience that end users love and organizations trust. Jamf is the only company in the world that provides a complete management and security solution for an Apple-first environment that is enterprise secure, consumer simple and protects personal privacy. To learn more, visit [jamf.com](https://www.jamf.com).



Lookout is a leading provider of endpoint and cloud security solutions. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and various partners across telecommunications and technology.

Powered by one of the largest sets of mobile code in existence, the Lookout Security Graph provides visibility into the entire spectrum of mobile risk. The installed base of Lookout's personal and enterprise mobile endpoint products is over 205 million mobile devices worldwide. This acts as a global sensor network that provides visibility into the threat landscape, including over 170 million apps—and that's growing by up to 90,000 apps a day. For more information, please visit [lookout.com](https://www.lookout.com).

