

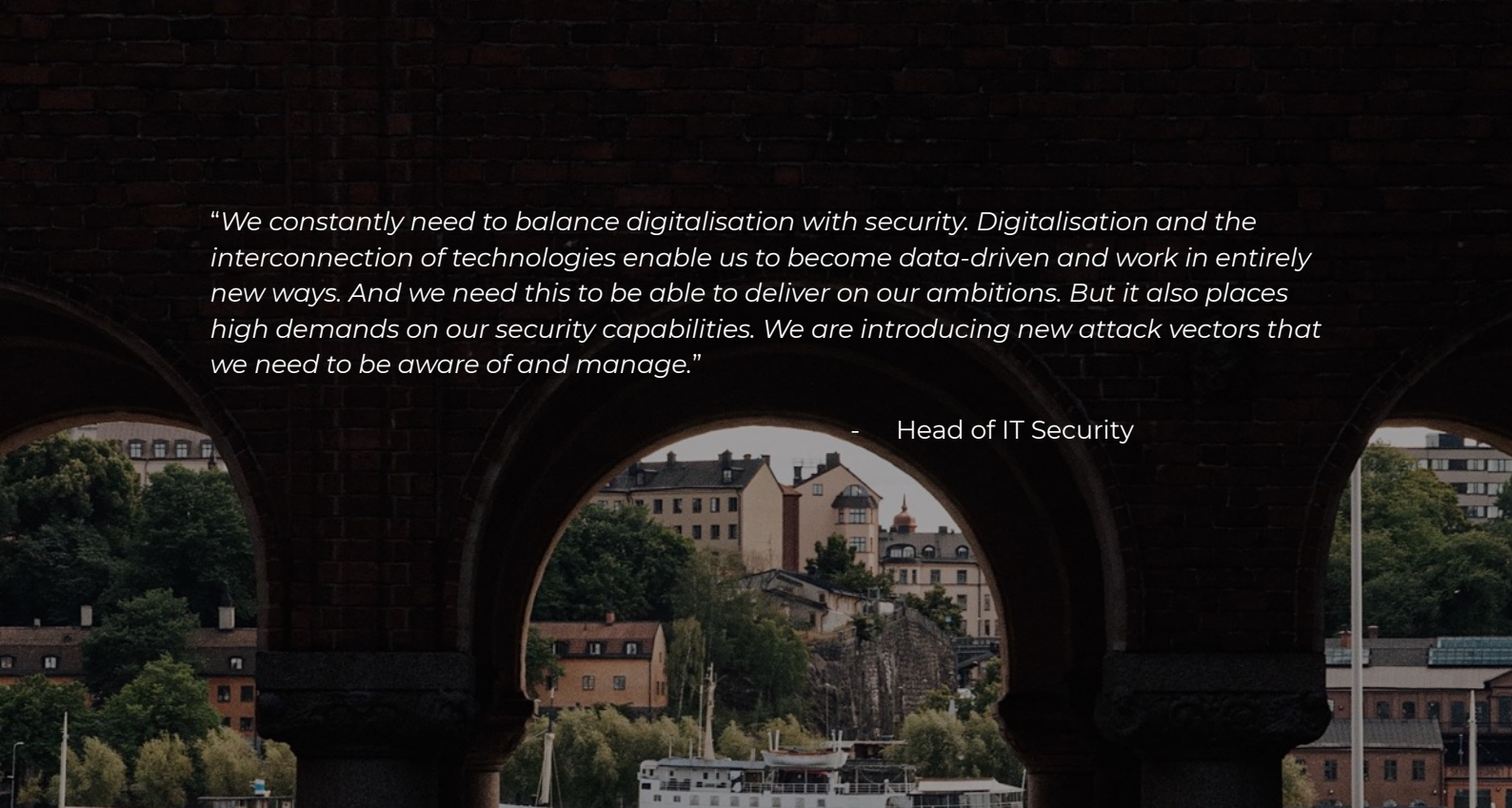


AVOKI

In collaboration with **Radar.**

SECURING THE MODERN WORKPLACE

CYBERSECURITY IN THE AGE OF
CLOUD, HYBRID WORK & AI



"We constantly need to balance digitalisation with security. Digitalisation and the interconnection of technologies enable us to become data-driven and work in entirely new ways. And we need this to be able to deliver on our ambitions. But it also places high demands on our security capabilities. We are introducing new attack vectors that we need to be aware of and manage."

- Head of IT Security

CONTENT

Executive Insights	3
Office Tech in the Modern Workplace	4
The New Reality	5
Threat Landscape	7
Organisational Challenges & Risks	10
Recommendations	15
References	19

ABOUT THE REPORT

Cybersecurity has become one of the defining challenges for modern organisations. This report examines the overlooked risks in office tech and explores how a new office reality of cloud, hybrid work, and AI are reshaping the threat landscape. Drawing on insights from the Nordic context and industry-specific perspectives, the report outlines key challenges both at a general level and within a few selected sectors - bank & finance, hospitality, healthcare & pharma, and professional services. It also provides recommendations for building resilience both broadly and tailored to these sectors.

The report has been prepared by Radar Group in collaboration with Avoki. All data points in the report are based on Radars own 2025 data, references to earlier studies are explicitly stated. Radar is solely responsible for the facts and conclusions presented in this report.

EXECUTIVE INSIGHTS

INSIGHT 1

THE WORKPLACE IS NOW A CYBER-PHYSICAL ECOSYSTEM

Modern workplaces blend cloud, collaboration tools, printers, Wi-Fi, meeting rooms, and IoT into one interconnected environment. Every device is a potential entry point, so office tech must be treated as part of the core security strategy.

INSIGHT 2

HYBRID WORK HAS PERMANENTLY EXPANDED THE ATTACK SURFACE

46% of Sweden's workforce now works from home at least part-time, double the pre-pandemic figures. 80% of security and business leaders believe this shift increases organisational risk.

INSIGHT 3

HUMAN FACTORS ARE THE FASTEST PATH TO COMPROMISE

Phishing, social engineering, and credential theft remain primary attack vectors, now supercharged by AI-generated content. Small mistakes enable lateral movement from "harmless" office tech to sensitive systems.

INSIGHT 4

THE OFFICE IS AN UNDERESTIMATED BLIND SPOT

Printers, conferencing gear, digital signage, and access systems often sit on flat networks with weak logging/monitoring and default configurations, yet they are connected (directly or indirectly) to important flows such as identity and information.

INSIGHT 5

AI REMAINS PERIPHERAL TO MOST CYBERSECURITY WORK

96% of Nordic organisations use or plan to use AI, yet only 41% apply it to cybersecurity. Of those, just 20% see it as a core function, while the rest treat it as a complementary add-on.

INSIGHT 6

MOST ORGANISATIONS OVERESTIMATED THEIR OT SECURITY

Only 29% believe that their office tech (printers, conferencing, signage, access systems) are sufficiently secured, leaving 71% exposed to potential exploitation.

INSIGHT 7

INDUSTRY RISK PROFILES DIFFER – BUT MATURITY GAPS PERSIST

Bank & finance and professional services have higher maturity but face blind spots in office tech and BYOD cultures. Healthcare and pharma grapple with highly sensitive data and complex OT environments, while hospitality struggles with distributed guest networks and low cyber awareness. Despite different risk contexts, weak governance, unclear ownership, and underestimated office tech remain common themes across sectors.

OFFICE TECH IN THE MODERN WORKPLACE

The modern workplace is no longer just desks, phones, and computers. It has become a digital ecosystem where cloud platforms, video conferencing systems, smart printers, wireless networks, and IoT devices are all interconnected. These technologies increase flexibility and collaboration, particularly in hybrid work models, by distributing access across multiple devices and locations.

At the same time, organisations are accelerating their digital transformation. As processes and workflows move to cloud and mobile environments, operational dependencies shift beyond traditional IT boundaries, exposing organisations to increased third-party and endpoint risks. This transformation unlocks significant opportunities for efficiency and innovation but also expands the attack surface in ways that traditional risk management can no longer address effectively. Despite this, office tech remains systematically underestimated as a security risk. Printers, conferencing tools, guest Wi-Fi networks, and other connected systems are often treated as peripheral assets, even though they are frequently outdated, misconfigured, or poorly monitored - and in many cases directly linked to core business systems.

Without clear ownership, proper segmentation, and security monitoring, these devices create blind spots that attackers can exploit to move laterally inside networks.

Cybersecurity is therefore no longer just a technical issue but a cornerstone of business continuity, trust, and resilience. Recognising how these structural shifts redefine the threat landscape is essential for building modern security strategies. The following sections explore this new reality in detail.

What is office tech?

Office tech refers to the connected technologies that support everyday office operations. Beyond traditional IT like servers and applications, it includes so-called “peripheral” systems - printers, conferencing tools, smart office devices, guest Wi-Fi, and even the building management systems, which are increasingly networked and potentially vulnerable.

Is your office security ready for the era of hybrid work?

THE NEW REALITY

The workplace has undergone fundamental structural changes in recent years. Hybrid work models and cloud-based delivery decentralize IT, increasing flexibility while reducing central control and policy enforcement. This shift expands the organisational attack surface, adding unmanaged endpoints and third-party dependencies. At the same time, rapid AI adoption is transforming both business operations and attackers' methods. Understanding these structural shifts is the starting point for strengthening organisational security.

The hybrid post-pandemic workspace

The Covid-19 pandemic forced workplaces to rapidly adapt, with many shifting to remote work. Years later, this hybrid model persists in 2024, 46% of employed people aged 20-64 in Sweden worked from home to some extent which is twice as many as before the pandemic¹. While hybrid work improved productivity and work-life balance, it also decentralised control, exposing organisations to new security risks, particularly around monitoring and endpoint management.

80% of security and business leaders believe they face greater risk today due to remote work²

These risks cluster in two areas. First, the hybrid workspace contributes to a decentralisation of the entire workspace, making it more difficult for IT teams to monitor and secure devices more effectively. Without physical access, policy enforcement and patching slow down, increasing time-to-remediate.

Second, remote workers are more exposed without office-based safeguards. Weak home networks and unsecured personal devices reduce protection levels, making phishing and malware attacks more likely³.

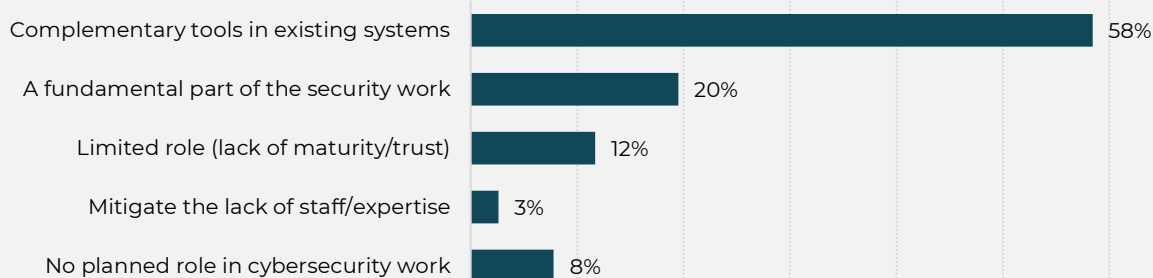
AI: a double-edged sword

AI is becoming deeply integrated into daily operations, and according to Radar's 2025 data, 96% of Nordic organisations already use or plan to use it. In cybersecurity, AI is a double-edged sword - it enhances detection and response but also introduces new vulnerabilities and governance challenges.

According to Radar's 2025 data, current use remains limited, focusing mainly on traffic analysis, automated triage, and threat intelligence platforms that process data at a scale no human can match. However, only 41% of organisations apply AI specifically to cybersecurity, compared with 70% for analytics - a clear sign that security adoption is lagging. Most (58%) use AI as a complementary tool, while just 20% treat it as a core component of their security strategy. This gap reflects a cautious stance: while AI's analytical potential is recognised, governance and data protection issues remain unresolved in many organisations. One reason for this cautious approach is that AI itself is viewed as a significant risk. Organisations see data privacy, protection, and governance as key AI risks that must be resolved before broader security integration.

83% of Nordic organisations see a high or moderate risk of misinformation when using AI
Source: Radar

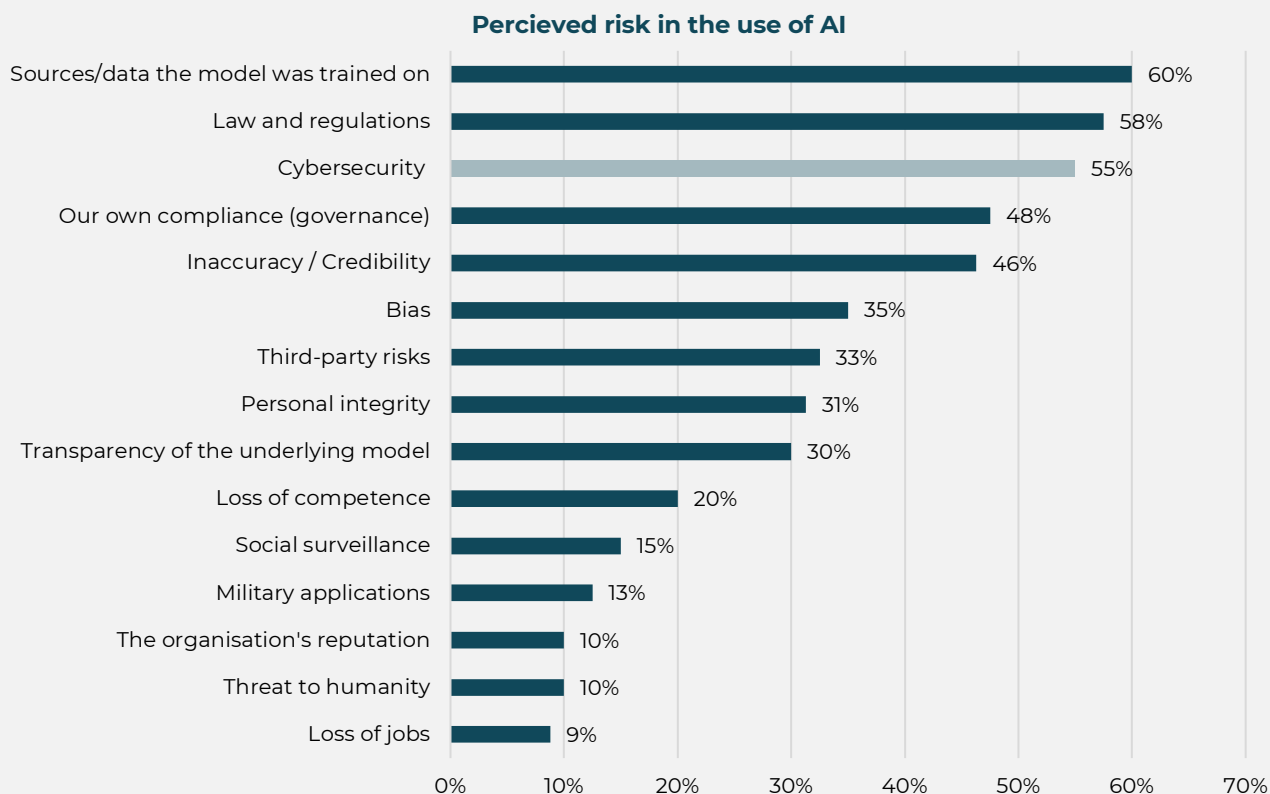
AI and machine learning in cybersecurity



¹ SCB (2025)

² Tenable (2021)

³ Telenor (2024)



Cloud-first, security second?

As office tech become increasingly cloud-connected, from document workflows to conferencing and collaboration platforms, the security perimeter extends far beyond the physical workplace. Understanding cloud dependencies is therefore essential to protecting the office environment as a whole.

Cloud technologies are at the heart of new delivery models and have enabled more flexible, scalable, and distributed workplaces. Platform technologies have contributed to a shift from fixed costs and owned infrastructure to a higher share of variable costs and operations. This has led many organisations to reduce their internal IT departments and in-house IT-expertise while becoming increasingly focused on procurement capabilities, supplier management, and sometimes maintenance and/or support.

However, with this shift organisations may have lost some operational technical capabilities. This may pose a security challenge when it comes to managing legacy office technologies if there are not enough resources or skills available.

Additionally, cloud-based businesses are also frequent targets for cybercriminals due to the vast amounts of sensitive data stored online, weak security practices, and the potential for large-scale disruptions - with almost half of security incidents reported to originate from cloud environments.

45% of security incidents reported to originate from cloud environments⁴

Addressing cloud security is therefore not just about securing external platforms, but about ensuring that governance, monitoring, and segmentation extend seamlessly across hybrid environments. Weaknesses in the cloud layer can undermine even well-secured office environments.

⁴ SentinelOne (2025)

THREAT LANDSCAPE

Recent geopolitical developments, particularly in Europe, have intensified the local threat landscape. State-sponsored actors and politically motivated campaigns increasingly target critical infrastructure, supply chains, and digital ecosystems, blurring the line between criminal and state-sponsored cyber operations. This evolving context puts additional pressure on organisations to build resilience against both opportunistic and coordinated threats. As workplaces evolve, threat actors adapt in parallel. ENISA, the European Union's cybersecurity agency, highlights emerging threats expected over the next five years⁵, of which three are especially relevant for office-related security.

Human error and exploited legacy systems in cyber-physical ecosystems

Connected infrastructure, OT, IoT, and smart devices will continue to increase and scale to improve efficiency and decision making. The widespread network of devices and nodes create security challenges in everything from maintenance, configurations, and end-user practices.

Advanced hybrid threats

Threat actors employ a variety of methods to achieve their goals. A combination of tactics, techniques, and procedures make hybrid attacks more difficult to defend against, and places high demands on detection tools to correlate and analyse different logs and events. These multifaceted campaigns overwhelm traditional detection tools, which rely on siloed telemetry.

Cybersecurity skills shortage

A lack of skills and knowledge is a cybersecurity challenge that is expected to continue in the coming years. The challenge is exacerbated by the interaction between new and legacy technology. Maintaining knowledge about risks and vulnerabilities in legacy systems, while at the same time understanding the impact on security posture from new technologies and emerging threats is a considerable challenge. This mismatch between legacy knowledge and emerging technology leaves critical gaps in defensive coverage.

ATTACKING EXAMPLES

Threat actors attack or tamper with equipment or devices to gain access and move laterally through networks to steal or manipulate data.

Threat actors combine digital and physical methods, targeting different vulnerabilities to avoid detection. Often deploying methods like social engineering, AI-enhanced attacks, and targeted phishing campaigns.

Threat actors gathering open and closed source information about the organisation, its technical environment, and its skillsets to identify deficiencies or vulnerabilities that can be exploited.

The emerging threats highlighted by ENISA illustrate how attackers increasingly target the structural complexities of modern workplaces. Hybrid environments that combine IT, OT, cloud, and office technologies create interdependencies that can be difficult to secure consistently. Threat actors exploit these weaknesses deliberately. Flat networks and weak integration points between IT and OT environments enable lateral movement, allowing attackers to escalate privileges and reach critical systems with minimal resistance. These vulnerabilities are often used as stepping stones in hybrid attacks, where initial access through cloud services or office tech leads to deeper infiltration.

⁵ Enisa (2023)

Real-world exploitation in the modern workplace

As workplaces become more digitally integrated, attackers increasingly target cyber-physical systems that bridge office technology, IT infrastructure, and cloud platforms. Organised cybercriminals with financial motivation are often opportunistic in their methods, actively scanning for known vulnerabilities and weak links across interconnected environments.

Today's workplaces often contain legacy or poorly monitored devices such as printers, conferencing systems, or smart office equipment that remain connected to core business systems. These assets are frequently underestimated as security risks and can be complex to protect due to legacy configurations, insufficient monitoring, and unclear ownership. Threat actors exploit precisely these conditions. Flat networks, unsegmented infrastructures, and limited visibility make it possible to move laterally once a single device is compromised. Treating office tech as peripheral or less critical than the rest of the IT stack therefore gives adversaries the foothold they need to initiate an attack and escalate impact. Several recent cases highlight how seemingly minor oversights in office tech or remote access can lead to significant organisational disruption.

Case: Misconfigured printer

A Nordic professional services firm experienced a data exposure incident when a networked printer cached sensitive client documents accessible via a public IP. The issue went unnoticed because the device wasn't part of central monitoring. The breach prompted a company-wide review of office device governance and segmentation.

Case: Remote work and credential theft

A midsize manufacturing company faced a ransomware incident after an employee reused a weak password on a personal device used for remote access. The attacker gained entry through the VPN, bypassing controls designed for on-site security.

Case: Supply chain disruption via misconfiguration in cloud services

A logistics company suffered a major service outage after attackers exploited a misconfigured cloud storage bucket belonging to a third-party vendor. The exposed credentials allowed access to shared office systems used for scheduling and tracking deliveries. The incident, which began as a supply chain compromise, ultimately halted operations for several days and demonstrated how interconnected infrastructures magnify the impact of even minor configuration errors.



HUMAN-CENTRIC PROCESSES ARE STILL THE WEAKEST LINK

As technical mitigation abilities are increasingly made available to the general public, cyber attackers increasingly exploit the human rather than just software vulnerabilities. Phishing, social engineering, and credential theft remain among the most common attack vectors, and in hybrid workplaces, the perceived distance between employees and centralised IT oversight only increases the risks. Humans are targeted because we are often easier to manipulate than systems. Attackers exploit pressure, distraction, and trust, with AI making phishing attempts ever more convincing.

Common human-centric risk scenarios in the office environment:

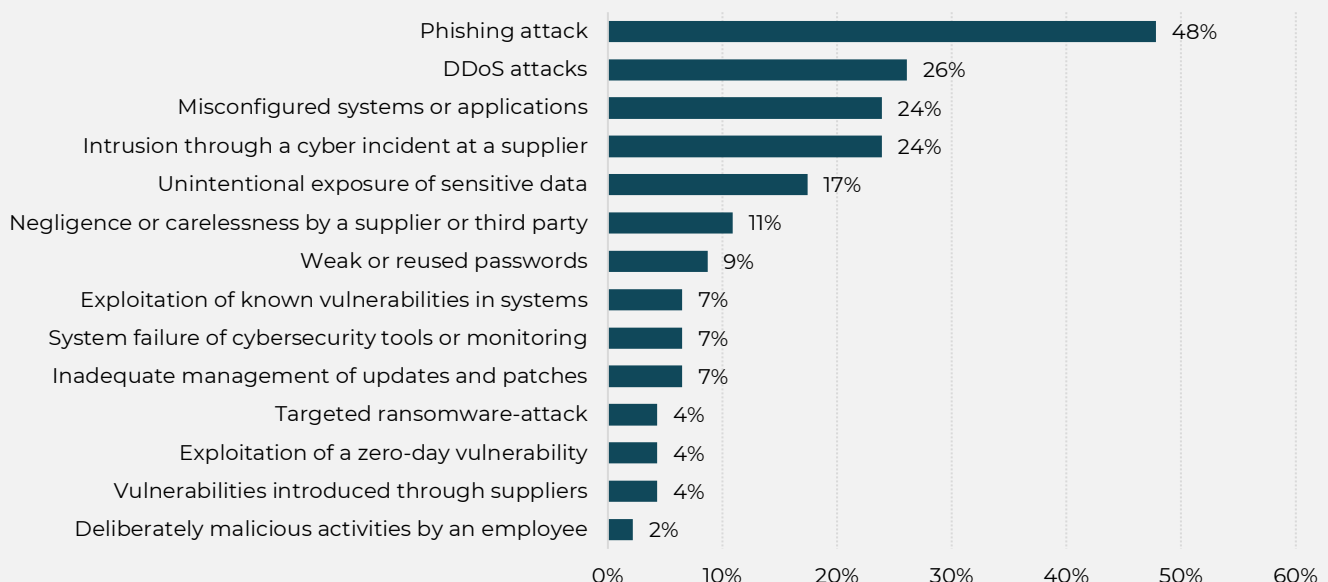
- A well-crafted phishing email on a personal device provides access to company systems unbeknownst to the user.
- Connecting an unapproved device to the office network, unknowingly exposing the network to malware.
- Conference room systems retain sensitive meeting recordings because no policy exists for deletion.
- Misconfigured printers or shared folders enabling data leakage.
- Unprotected digital signage or smart office devices are connected on flat networks, providing entry points.
- Misconfigured cloud storage exposes sensitive business data, with no backup or monitoring to detect the breach.
- Sharing confidential information into a public AI tool, creating regulatory and compliance risks.

Even seemingly small mistakes can lead to major breaches when attackers are able to pivot from one compromised endpoint to more sensitive internal systems. That is why improving the human aspect of cybersecurity is both necessary and urgent.

Making the secure path the default path

An effective approach to office cybersecurity is to integrate user behaviour and awareness as part of system design. That means embedding protection into the architecture of systems and processes rather than relying on user vigilance. This includes applying least privilege access, setting secure defaults for office tech, and enforcing network segmentation so that a compromised device cannot provide attackers with broad access. Equally important is monitoring and logging, which allow unusual behaviour to be detected early. By making the secure path the default path, organisations reduce reliance on perfect behaviour and create an environment where errors are expected, contained, and recoverable.

Primary causes of cyber incidents



ORGANISATIONAL CHALLENGES AND RISKS

Different sectors face unique operational contexts, regulatory pressures, and technology landscapes, which shape specific risk profiles. Recognising and addressing these sectoral differences is critical for designing targeted measures that move beyond one-size-fits-all security strategies.

However, cybersecurity challenges in office environments span both universal and sector-specific dimensions. Broad threats such as phishing, ransomware, and data breaches affect nearly all organisations and must be addressed as a security baseline.

Cross sector challenges and risks

As organisations integrate physical and digital assets, offices become more data-driven and efficient - but also more complex to secure, with risks shifting from isolated IT systems to interconnected ecosystems.

It is common to view traditional office technology as single purpose “dumb” products and to underestimate complexity and potential security risks. As previously stated, we should now be aware that the workspace includes all kinds of connected systems, directly or indirectly, linked to core business systems. Office technology is often handling sensitive information and include capabilities that require internet access for full functionality. Another challenge is a lack of visibility and unclear responsibilities, as some of these systems have traditionally been a part of the facilities domain and IT has not always been included in the process of acquiring them.

Organisations are generally focusing their security efforts on revenue-generating assets, such as servers or applications, underestimating the risk of office technology becoming an entry point. In our inter-connected world, most entry points are equally valuable for the antagonist.

Security efforts risk becoming siloed when office technology is left out of the monitoring and logging ecosystem that is applied to other core technologies. These organisational gaps are compounded by structural weaknesses. Many organisations still run flat or poorly segmented networks, where office tech, IT, and OT share infrastructure without proper isolation. In essence, undermining perimeter defences and allowing threats to move freely between office devices and critical systems, amplifying the impact of a single misconfiguration or compromise.

31%

Security monitoring leads, print security lags - only a third make it a priority

Source: Radar

DIGITAL WORKPLACE AREAS

COMMON RISKS

Connected technologies in office environments

- Flat networks
- Lack of visibility of connected devices or endpoints
- No/limited logging from printers or other office technology to SIEM-tools
- Lack of/insufficient segmentation

Document management

- Misconfigured printers
- Data exposure or leaks
- Unattended printing of sensitive materials

Collaboration platforms

- Unprotected meeting links
- Incorrect sharing rights
- Voice or meeting recordings

Meeting and smart office technology

- Recordings without lifecycle management
- Digital signage without proper segmentation

IT infrastructure

- Insufficient protection for east-west traffic (internal network traffic between devices/systems)
- Default configurations
- Vulnerable firmware and insufficient update cycles

Cloud services and IT operations

- Misconfigured cloud applications
- Lack of or insufficient backups
- Limited monitoring and logging

AI technologies

- Incorrect data management
- Lack of governance and control
- Regulatory and compliance issues

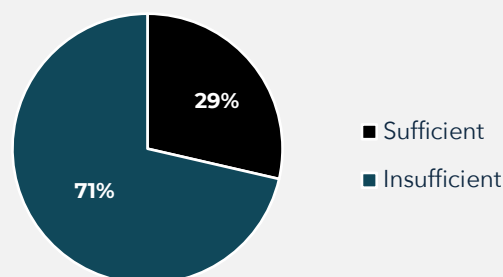
Insufficient level of security

Despite the critical role that office technology play in daily operations, only 29% of organisations believe their cyber-physical systems are sufficiently secured, according to Radar's 2025 data. This leaves as many as 71% exposed to potential threats, many of which stem from underestimated risks within office environments. This reflects the broader industry trend, where many organisations struggle to extend mature cybersecurity practices beyond traditional IT to include connected office technologies. These risks are often overlooked because office tech such as printers, video conferencing equipment, and guest networks is still viewed through an "IT outlying" lens rather than as part of a wider ecosystem. Moreover, many organisations lack the foundational structures needed to manage these systems securely, which often leads to reactive efforts.

Addressing these gaps requires not just recognition of the problem, but structured action to build resilience.

The barriers to achieving adequate security in these systems also help explain the gap. As the figure below shows, organisations cite lack of internal knowledge, leadership, and limited budgets as the most critical challenges. In the office context, this translates directly to everyday technologies: printers without logging, conferencing systems with insecure defaults, or flat networks. Without clear ownership or sufficient investment, office tech remains one of the easiest ways for attackers to gain a foothold and one of the hardest areas for organisations to prioritise protecting.

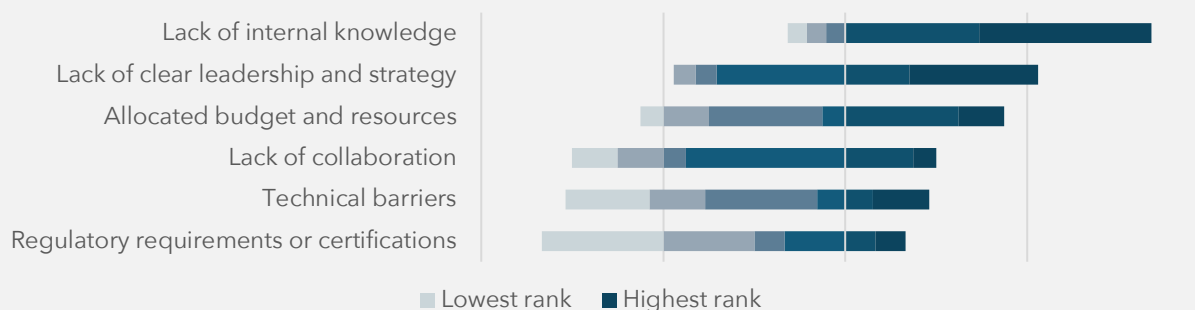
Security in cyber-physical systems



Outsourcing and the "knowledge gap"

As many organisations rely on outsourcing to manage its IT environments, internal teams are often left operating under challenging conditions. Small in size but responsible for an ever-growing range of systems and suppliers. The most cited barrier to security is lack of internal competence. When core functions are delegated externally without sufficient internal capability to oversee or challenge them, organisations risk losing visibility and control. For smaller IT departments, this can mean that office tech security, perceived as low risk, simply falls down the list of priorities. Indeed, scarce resources require tough priorities. To close the gap, management must recognise the growing complexity of IT operations and ensure teams have the resources and mandate to secure the entire environment, including office tech.

Main barriers to achieving adequate security in cyber-physical systems



Sector-specific challenges and risks

Examining sectors such as banking & finance, hospitality, healthcare & pharma, and professional services is essential, as they face complex cybersecurity challenges. These industries handle large volumes of sensitive data and provide critical services that underpin economic stability and societal well-being, making potential disruptions far-reaching. Using **Radar's 2025 data**, the following section explores the key IT and cybersecurity priorities and challenges for each sector.

BANKING & FINANCE

The banking and finance sector has a high digital maturity, as well as a high cybersecurity maturity, partly due to being a heavily regulated sector. Having been at the forefront of digitalisation, many organisations are now struggling with a technical debt and operating legacy systems. Cybersecurity is both a top priority and challenge in this sector, along with regulatory compliance, but office tech could be a potential blind spot for security. Banking and finance organisations are taking the lead in implementing AI and see it as a fundamental part of the security work to a higher degree than other sectors. The combination of emerging technologies and legacy systems can pose security challenges that need careful attention.

POTENTIAL RISKS

- An aging and decreasing talent pool for legacy systems.
- Meeting infrastructure such as voice and video equipment recording sensitive discussions.
- Misconfigured printers or other office equipment in local branch offices.
- Data leaks from AI-use without clear policies.

IT-STRATEGIC PRIORITIES 2025

1. Strategic cybersecurity
2. Compliance and governance
3. Automation

IT-STRATEGIC CHALLENGES 2025

1. Strategic cybersecurity
2. Technical cybersecurity
3. Cybersecurity training and knowledge transfer

HOSPITALITY

Issues surrounding automation and digitalisation are the key IT priorities and challenges within the hospitality sector. While the importance of cybersecurity is recognised as a key IT-priority, it is not identified as a strategic IT challenge. Organisations within the hospitality sector operates under strict regulations as large volumes of personal data is handled. Ensuring compliance can be particularly challenging due to the sector's typically high staff turnover, making it more difficult to keep everyone up to date on security protocols. Mirroring this, Radar's data shows that a key cybersecurity priority is improving employees' knowledge and awareness about cybersecurity. While the top challenges include limited internal relevant competence, resistance to change in one's own operations, and lack of commitment from management.

POTENTIAL RISKS

- Network configurations, encryption, and authentication vulnerabilities, including guest wi-fi as a potential entry point.
- High employee turnover and lack of cybersecurity awareness among staff.
- Not a traditionally tech focused sector and focus on guest experience may outweigh security considerations.

IT -STRATEGIC PRIORITIES 2025

1. Strategic cybersecurity
2. Automation
3. Changing operating and business models

IT-STRATEGIC CHALLENGES 2025

1. Automation
2. Changing operating and business models
3. Understanding and managing digital business risk

HEALTHCARE & PHARMA

The healthcare and pharmaceutical sector manages highly complex environments of operational technology, including office-related systems and document management platforms. At the same time, these organisations handle extremely sensitive personal data, alongside research, development, and intellectual property that make them attractive targets for cyberattacks. While the industry is subject to strict regulatory frameworks, it is relatively inexperienced when it comes to implementing and complying with cybersecurity-specific regulations. This creates a dual challenge: protecting critical data assets while navigating a regulatory landscape that is rapidly evolving. The sector's combination of sensitive information, interconnected systems, and regulatory immaturity requires focused investment in governance, monitoring, and secure design to reduce risk exposure.

POTENTIAL RISKS

- Meeting infrastructure such as voice and video equipment recording sensitive discussions.
- Printing of sensitive patient and/or research data.
- Specialised and interconnected medical equipment and devices creating a wide attacking surface and potential for unauthorised access by lateral movement through networks.

IT-STRATEGIC PRIORITIES 2025

1. **Strategic cybersecurity**
2. **Automation**
3. **Increased automation rate**

IT-STRATEGIC CHALLENGES 2025

1. **Automation**
2. **Changing operating and business models**
3. **Management of existing applications**

PROFESSIONAL SERVICES

Professional services is a broad sector that includes firms offering specialised knowledge to clients, such as law firms, audit and accounting firms, engineering services, and HR consulting. Although these operate in diverse fields, they face similar challenges in their cybersecurity efforts. They are typically knowledge-intensive firms and attractive targets for cyberattacks due to their handling of sensitive and customer data. At the same time, trust is fundamental to their organisational reputation, as clients expect professionalism, precision, and technological capabilities. In general, businesses within this sector demonstrate high levels of digital and cybersecurity maturity, driven by regulatory requirements and the need to maintain client trust. However, some also struggle with outdated or fragmented technology, limited internal IT resources, and a BYOD (bring your own device) culture.

POTENTIAL RISKS

- Management of business documents.
- Conference and meeting rooms with equipment sensitive to recordings/external access.
- Data loss, unauthorised access, unsecure network connections, or compliance issues stemming from a BYOD culture.

IT -STRATEGIC PRIORITIES 2025

1. **Strategic cybersecurity**
2. **Automation**
3. **Changing operating and business models**

IT-STRATEGIC CHALLENGES 2025

1. **Strategic cybersecurity**
2. **Automation**
3. **Changing operating and business models**

71%

of organisations that lack a secure cyber-physical environment most often cite limited internal knowledge, unclear leadership, and constrained budgets as the main barriers.

29%

of organisations believe their cyber-physical systems are sufficiently secured.

“Security isn’t lost in the cloud or the datacentre - it’s lost in the everyday systems no one owns.”

RECOMMENDATIONS

Closing the gaps in office tech – from blind spots to resilience

The modern workplace has never been more connected, or more exposed. Hybrid work, cloud adoption, and the rise of AI have transformed efficiency and collaboration but have also created new vulnerabilities that traditional IT security was never designed to handle. Office tech, from printers and conferencing tools to smart devices and cloud applications is still all too often treated as peripheral, despite being directly linked to core business systems. The antagonists do not care about the business value of each entry point if it enables lateral movement in the environment.

This gap is costly. Misconfigured devices, unsecured meeting platforms, and unmanaged document flows create entry points that attackers can exploit to move laterally into sensitive environments. Meanwhile, many organisations struggle with legacy systems, outsourcing dependencies, and unclear ownership structures. The result is uneven security maturity, with critical blind spots persisting in daily operations.

The opportunity, however, is clear. Acting now can turn these weaknesses into strengths by embedding visibility, governance, and resilience into our office environments. This approach not only reduces exposure but also strengthens compliance, and more importantly builds trust internally as well as externally.

Strategic priorities

To address these challenges effectively, we must move beyond tactical fixes and adopt a holistic approach that integrates leadership, competence, and secure design with robust technical safeguards. This involves acting on several fronts simultaneously:

- **Establish clear governance and ownership** of office technologies, aligning responsibilities across IT, facilities, and vendors.
- **Secure document flows, collaboration platforms, and smart office technologies by default**, reducing reliance on manual controls.
- **Build resilience** through infrastructure hardening, cloud continuity, and AI governance to ensure that everyday technologies do not become single points of failure.

By addressing these areas strategically, organisations can close their most overlooked security gaps and build a workplace environment that is secure, innovative, and resilient.



The value of doing things differently

Engineering security into office environment reduces incident impact, raises customer trust, and improves regulatory posture. Organisations that move beyond reactive, compliance-only approaches gain a real advantage: stronger protection against disruption, greater customer confidence, and a more credible position with regulators.

Addressing the challenges

The organisational challenges outlined earlier require structured action, beginning with visibility. We need an accurate inventory of connected assets, from printers and meeting systems to smart signage and conferencing tools. Effective protection also depends on strong internal boundaries. Many office environments still lack proper network segmentation, allowing threats to spread once inside. Clear network separation with proper monitoring and governance helps contain risks and prevent small errors from becoming major incidents.

Capabilities of higher maturity

A mature security approach to office IT and the broader digital workplace can be recognised by a set of core capabilities:

1. **Governance and ownership:** Clear responsibility for office IT security, with aligned processes across IT, facilities, and vendors.
2. **Secure document workflows:** Printing and document flows monitored and protected to avoid data leaks, misconfigurations, or unmonitored output.
3. **Protected collaboration:** Securely configured conferencing and telephony platforms protect sensitive conversations and recordings.
4. **Smart safeguards:** Meeting technology and smart office solutions governed by lifecycle policies, with recordings and signage protected from unauthorised access.
5. **Infrastructure resilience:** Strong protection in datacentres, secure configurations, and ongoing firmware and patch cycles.
6. **Cloud security and continuity:** Cloud applications configured correctly, with backup, monitoring, and resilience measures integrated into operations.
7. **AI governance:** AI systems deployed with clear guidelines for data use, transparency, and compliance, reducing risks of bias, data leakage, or regulatory breaches.

Leadership and collaboration

Security can no longer be left to IT alone. It requires visible leadership commitment to prioritise resources, allocate budgets, and foster a security-first culture. True resilience is built when IT, facilities, and business units work together to close functional gaps. Investments must extend beyond technology into skills and competence, while reducing over-reliance on outsourcing to ensure organisations can respond swiftly and decisively to incidents.

Technical measures that make a difference

Organisational change requires solid technical safeguards, including:

- **Least privilege** limits users to only what they need, while multi-factor authentication (MFA) adds a critical safeguard against stolen credentials.
- **Lifecycle management of devices** from printers and conferencing tools to IoT equipment, keeps firmware and configurations secure and up to date.
- **Zero-trust principles** applied to hybrid and BYOD environments prevent unauthorised lateral movement, even if a device is compromised.
- **Harden core infrastructure** through consistent patch cycles, configuration baselines, and isolation of critical assets. A secure office environment depends on the resilience of the underlying infrastructure it connects to.
- **Strengthen cloud security** through consistent configuration reviews, identity and access controls, and monitoring of third-party integrations.
- **Network segmentation and east-west traffic inspection** to limit lateral movement between office tech, IT, and OT environments. Proper isolation reduces the blast radius of any single compromise.
- **Integrated monitoring and logging** provide visibility, with events from office tech feeding into SIEM platforms for early anomaly detection.
- **Clear incident response playbooks** that include office technologies and cloud environments, supported by regular scenario-based exercises. Integrating these assets into response routines shortens detection and containment times.
- **Scenario-based testing**, and office tech-focused penetration exercises prepare organisations to detect and respond to real-world threats.

Building resilience for the future

Technical safeguards such as network segmentation, lifecycle management, and continuous monitoring remain essential foundations of office security. Yet true resilience requires more than tools, it demands leadership, collaboration, and an embedded security culture that extends across every layer of the organisation.

Organisations that invest in visibility, governance, and secure design will not only reduce risk but also strengthen operational continuity and client trust. As workplaces evolve through hybrid models, cloud adoption, and AI integration, securing the office environment is no longer optional.

Security built into everyday systems, not added later, will define the resilient and competitive organisations of tomorrow.



Sector-specific summary

While many of the challenges around office IT are shared across sectors, the risks manifest differently depending on maturity, regulation, and business models. This makes a one-size-fits-all approach ineffective. The following industry-specific guidance highlights where to focus efforts to close the most critical gaps and strengthen security maturity.

INDUSTRY	STRATEGIC RECOMMENDATIONS	TECHNICAL RECOMMENDATIONS
Bank & finance	<ul style="list-style-type: none">- Integrate administration IT explicitly into governance and compliance frameworks.- Regularly assess OT alongside IT in audits.- Reduce dependency on ageing legacy expertise through structured competence development.	Apply zero-trust segmentation to office networks; enforce lifecycle management (patching, firmware updates) for printers and conferencing tools; enable logging and monitoring of meeting platforms to detect unusual access to sensitive discussions.
Professional services	<ul style="list-style-type: none">- Strengthen data governance with clear ownership for document flows and collaboration tools.- Implement security awareness programmes focusing on client confidentiality and insider threats.	Secure print environments with monitoring; enforce MFA and conditional access for collaboration platforms; segment BYOD devices from core systems; apply logging to conferencing/AV systems.
Health & pharma	<ul style="list-style-type: none">- Establish a cross-functional security steering group to align IT, OT, and compliance.- Build internal competence on Office IT to reduce dependency on external vendors.	Enforce secure defaults for print and document workflows; segment medical and office networks; monitor remote vendor access with strict authentication; integrate OT logs into SIEM.
Hospitality	<ul style="list-style-type: none">- Build a culture of cybersecurity awareness adapted to high turnover environments (short, scenario-based training).- Assign clear ownership for Office IT across IT and operations.	Enforce network segmentation between guest Wi-Fi and operational systems; apply encryption/authentication to all access points; enable PoS monitoring for anomalies; implement managed print/document security in distributed sites.

Across industries, the nature of risk varies, and so do the priorities for action. What they all share, however, is that office technology rarely receives the same attention as traditional IT. Everyday systems such as printers, conferencing platforms, guest Wi-Fi, and smart office devices are still seen as conveniences rather than critical assets. Closing this gap requires more than isolated technical fixes. It means embedding office technology into the broader security strategy, supported by clear governance, defined ownership, and sustained investment in competence. When combined with practical safeguards such as segmentation, monitoring, and secure configuration, these measures can transform office technology from an overlooked weakness into a controlled and resilient part of the organisation's digital ecosystem.

Cybersecurity is only as strong as its most overlooked link, and for many organisations, that's office tech.

EXTERNAL REFERENCES

ENISA (2023). Foresight Cybersecurity Threats for 2030.
<https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>

SCB (2025). Fler jobbar mer hemifrån.
<https://www.scb.se/pressmeddelande/fler-jobbar-mer-hemifran/>

SentinelOne (2025). 17 Security Risks of Cloud Computing in 2025.
<https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/>

Telenor (2024). 17.7 Million Scam SMS Messages Blocked in Q1 2024. Available at: <https://www.telenor.no/om/sikkerhet/>

Tenable (2021). Seventy-Four Percent of Organizations Attribute Damaging Cyberattacks to Vulnerabilities in Technology Put in Place During the Pandemic, According to Global Industry Study <https://www.tenable.com/press-releases/seventy-four-percent-of-organizations-attribute-damaging-cyberattacks-to>

