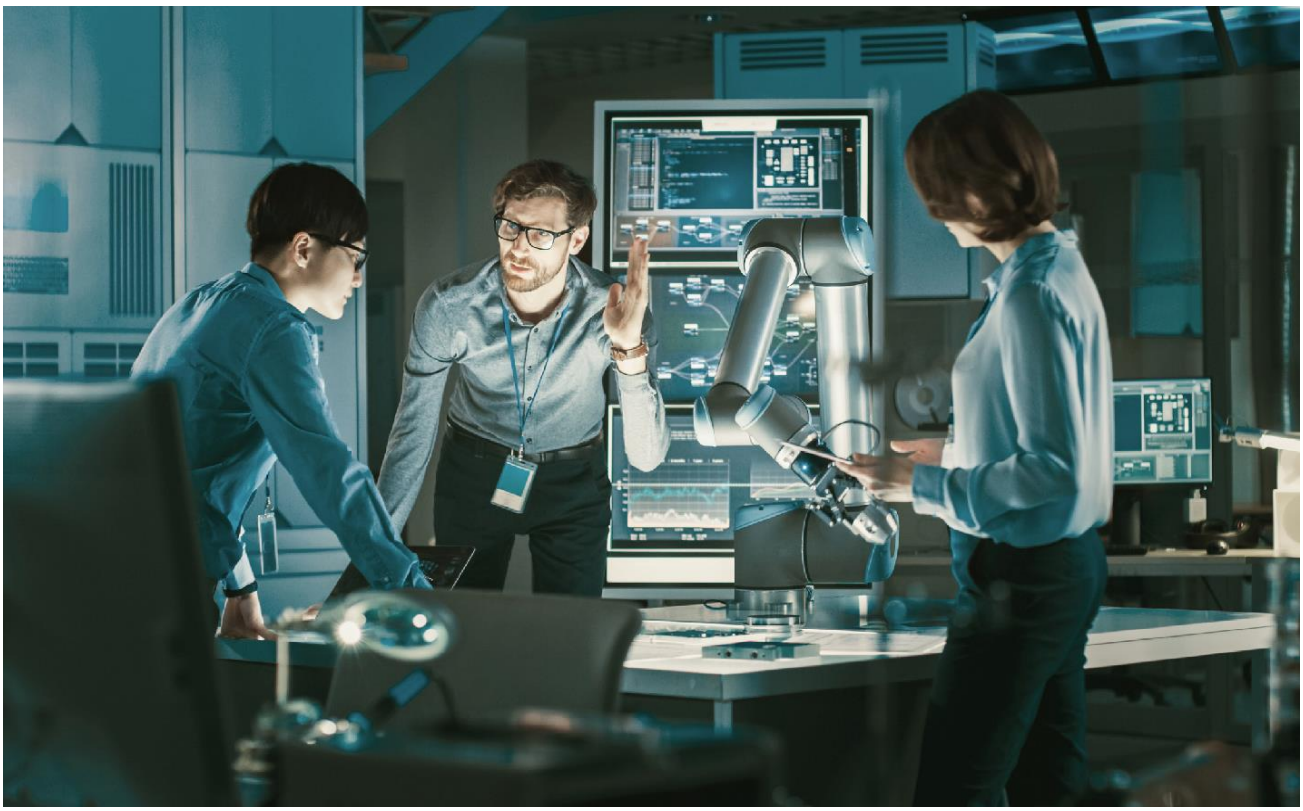
Report 2022

# IT Security Economics 2022

## Executive summary



kaspersky BRING ON THE FUTURE

kaspersky.com

# IT Security Economics 2022

After two years of pushing beyond traditional business models highlighted in the 2021 IT Security Economics Report, businesses have continued to face the additional challenges of leading their organizations through further uncertain waters.

General cybersecurity trends are pushing organizations into a proactive position as they now have to protect themselves under conditions of rapid digitalization, and skills shortages amid continuing geopolitical and economic uncertainty.

The biggest headache for IT managers is how to protect their organization in 2023 and beyond, as they focus on securing business processes from cyber intrusion, requiring increased security budgets over the next three years, by up to 14 %.

Our research also reveals IT security teams are now battling data leakages caused by employees almost as frequently as breaches caused by cyberattacks, following the introduction of new staff laptops or tablets, and Virtual Private Networks (VPNs) to enable remote working last year.

This year we found there has also been a shift in the mindsets of organizations as many transitioned certain functions to outsourced services such as managed service providers (MSP) and managed security service providers (MSSP) to find more efficient ways of delivering cybersecurity solutions. This compares to a year ago, when IT managers were considering the potential transition to cloud servers and collaboration software.

## Methodology

The Kaspersky Global Corporate IT Security Risks Survey is an annual study into the state of IT security within organizations across the world

This study includes interviews from a total of 3,230 respondents working in businesses of various sizes from small to medium businesses with more than 50 employees through to major corporations. It was conducted across 26 countries in the major B2B markets where Kaspersky Lab operates.

Throughout the report, businesses are referred to as either SMBs (small and medium sized businesses with 50 to 999 employees), or enterprises (businesses with over 1,000 employees).

# Key findings

Cybersecurity incidents with the most impact in terms of costs and efforts affected **IT infrastructure hosted by a third party for SMBs** and **targeted attacks for enterprises.**

Cybersecurity budgets in 2022 averaged **$3.75m to enterprises** and **$150k to SMBs**. Both segments are planning to increase budgets equally up to **14 percent** in the coming year.

**Communications, product development and customer support** are the top three processes most affected by cybersecurity intrusions.

**Data leaks** were the most encountered security issue this year. This type of incidents most often **was caused by employees (22%) and attackers (23%).**

**Delivering cybersecurity solutions and efficiencies by bringing in external experts** are **the main drivers** leading companies to outsource IT security.

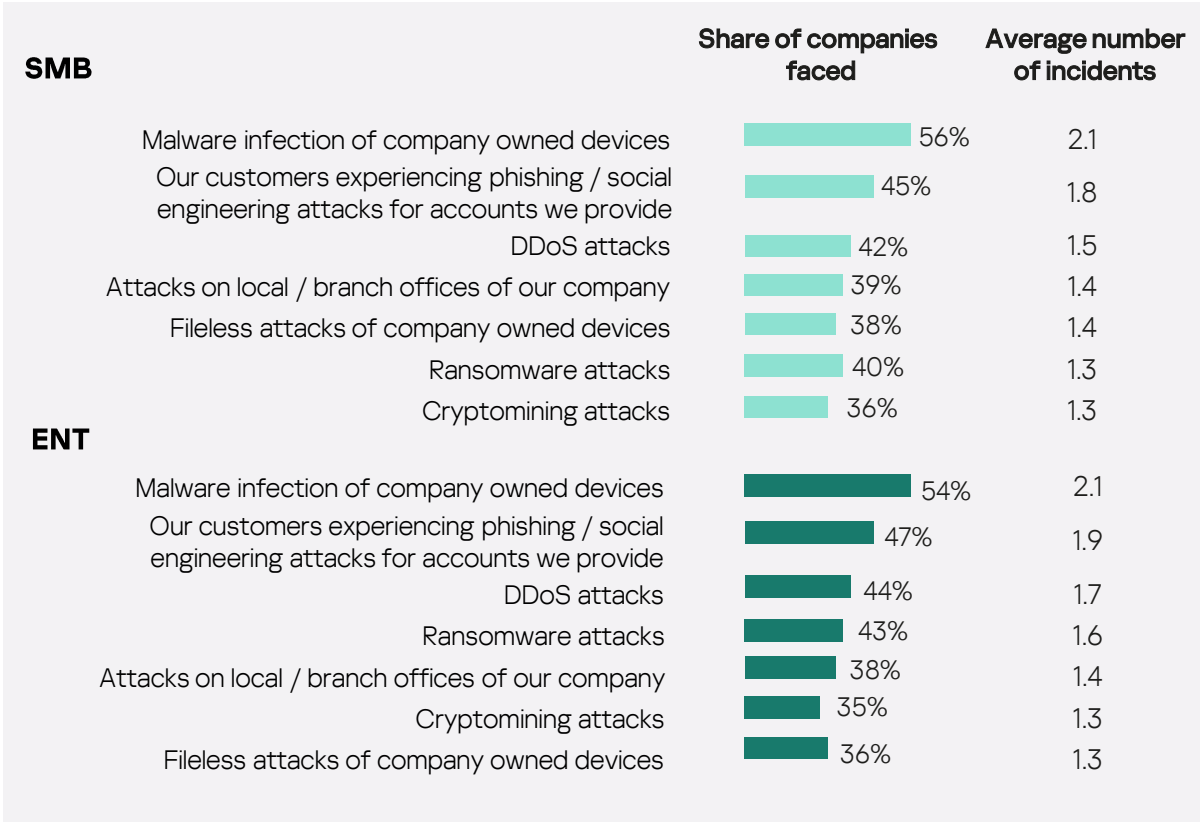
## New obstacles with the same challenges

In addition to navigating and building resilience to new business obstacles in the face of seemingly unrelenting disruptions, cybersecurity risks have this year continued to be a big concern for enterprises and small businesses.

Malware infection and phishing attacks on customers' accounts appear to be the top threats companies faced in 2022.

In fact, SMBs faced an average of two attacks a year, a situation that draws the same picture in the enterprise segment.

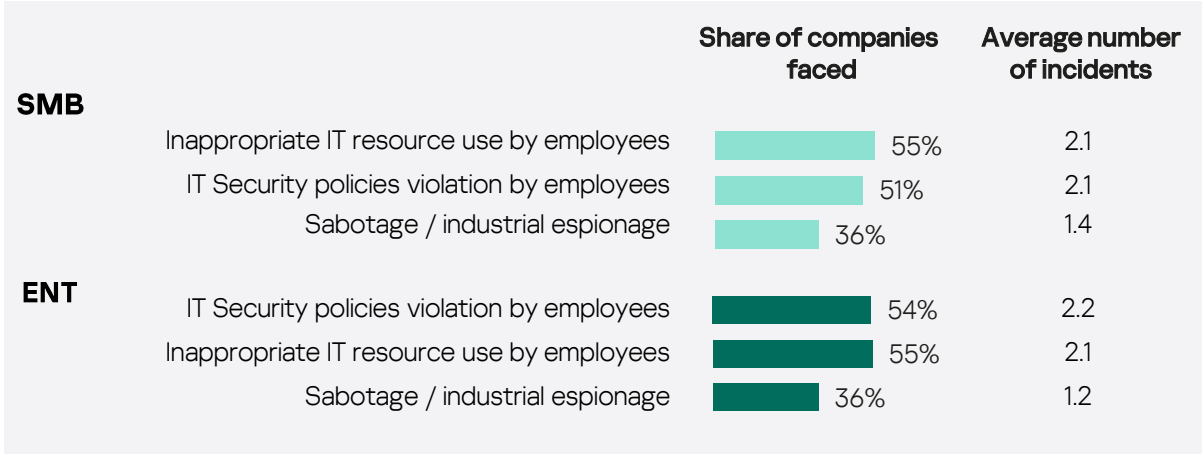
## Threats & Concerns: Business continuity




In 2022 IT security managers have faced cyber threats caused not only by external cyber criminals trying to penetrate the company's systems, but also by employees violating IT Security policies.

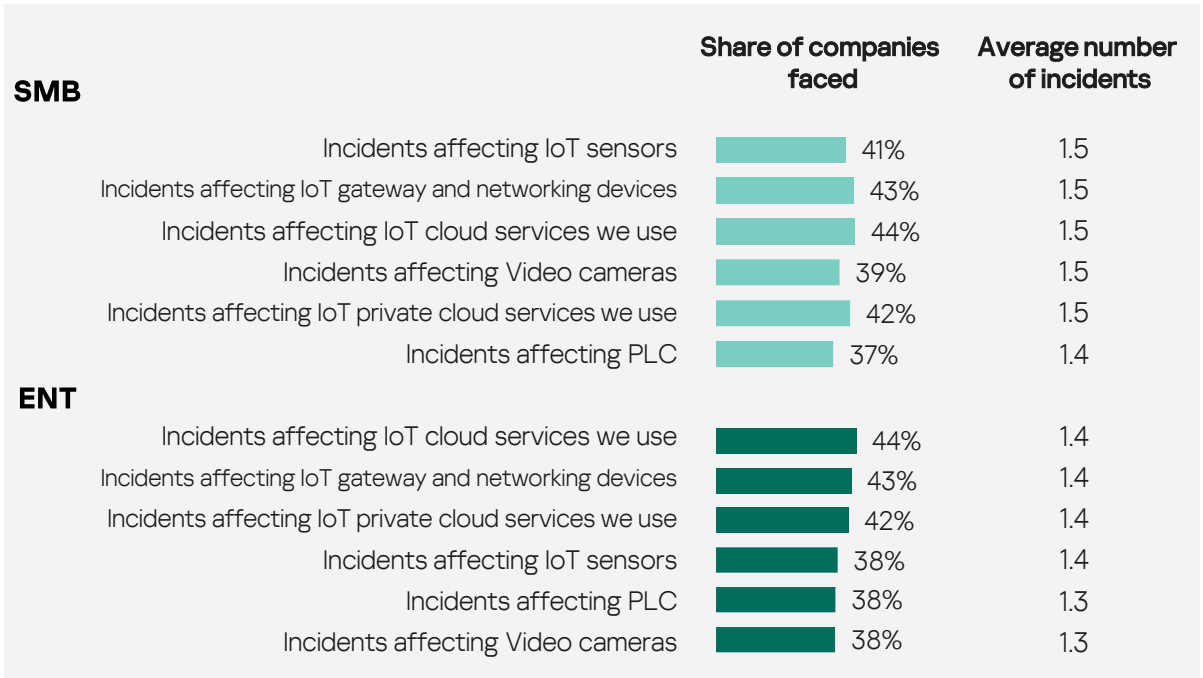
Fifty five percent of corporations faced IT Security policy violations by their own employees.

## Threats & Concerns: Ensuring staff compliance




Smart devices used at home and in the workplace such as digital personal assistants and web-enabled lightbulbs have become commonplace, but they are also a gateway for cyberattacks for both SMBs and enterprise customers. Companies faced an average of two incidents in 2022, affecting IoT sensors, IoT cloud services and IoT networking devices.

## Threats & Concerns: Security issues of IoT infrastructure



## Data protection and cybersecurity breaches

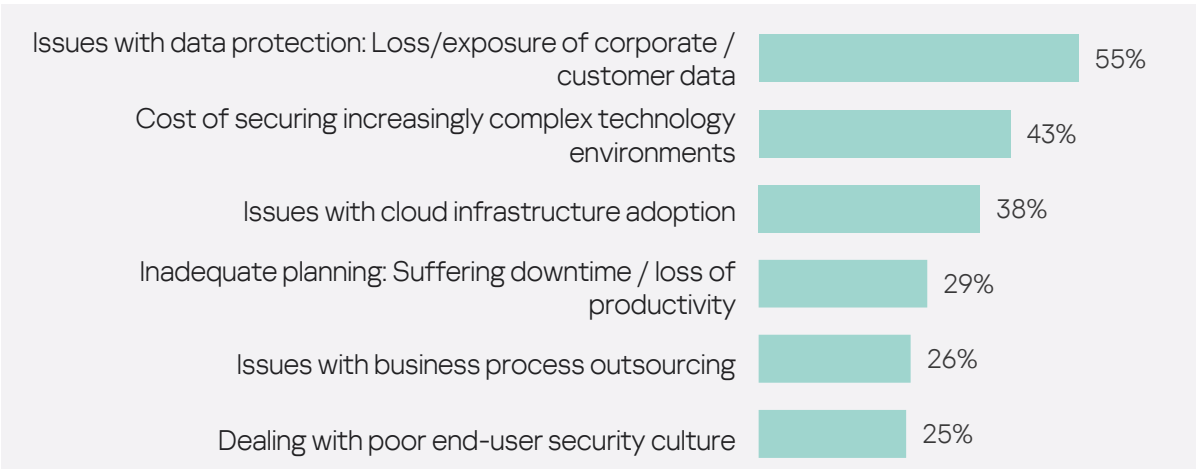
Data protection is still the biggest business security concern, whether you're a mom-and-pop store or a large corporation. Respondents reported data breaches via internal systems caused by cyberattacks and employees.

Yuliya Novikova, Head of Security Services Analysis at Kaspersky, advises on how data breaches can be a growing risk for companies due to the following factors and reasons:

1. When compromised company data appears in public, it may be of interest to cybercriminals, so they can use it for phishing and social engineering attacks.
2. Cybercriminals are expanding their social media presence and now publish information on successful attacks against victims to Twitter accounts, personal websites and public messengers. This creates serious reputational risks for companies and individuals, because even a fake statement can create a wider social media discussion and manipulate public opinion.
3. The risks of a data breach increase if they involve leakage of PII (personally identifiable information), as it could result in serious reputational and financial losses, and possible GDPR fines for breaking data protection rules - companies may also incur legal fees if they face litigation.

This year, just over half (55%) of companies consider issues with data protection to be the most challenging.

The second most important concern highlighted by 43% of respondents was the cost of securing increasingly complex technological environments, while issues with cloud infrastructure adoption followed (38%).



# Transparency becoming increasingly pervasive

Increased attention to transparency polices is one of the results of concerns about data protection and - as a result - has become a big security issue for business as more importance is placed on the transparency policies of suppliers and contractors.

The common concern is the approach by stakeholders toward data management, accompanied by a wider adoption of such policies by these organizations themselves.

A total of 91% of respondents consider the presence - or absence - of transparency policies is important when considering doing business with a supplier or contractor, with enterprises and SMBs considering it equally important. The APAC region pays most attention to the issue with the majority of businesses — 98% — saying they are a major consideration when considering a supplier or contractor.


Kaspersky has been a pioneer in building digital trust in the cybersecurity industry, having launched the Global Transparency Initiative (GTI) to provide its stakeholders with greater visibility into how the company and its solutions work. The GTI serves as an actionable framework for validating and verifying the trustworthiness of the company's products, internal processes and business operations. Since its launch in 2017, the initiative has grown in scope to include a number of actionable and unprecedented measures – for instance, source code reviews – and set an industry benchmark for transparency.

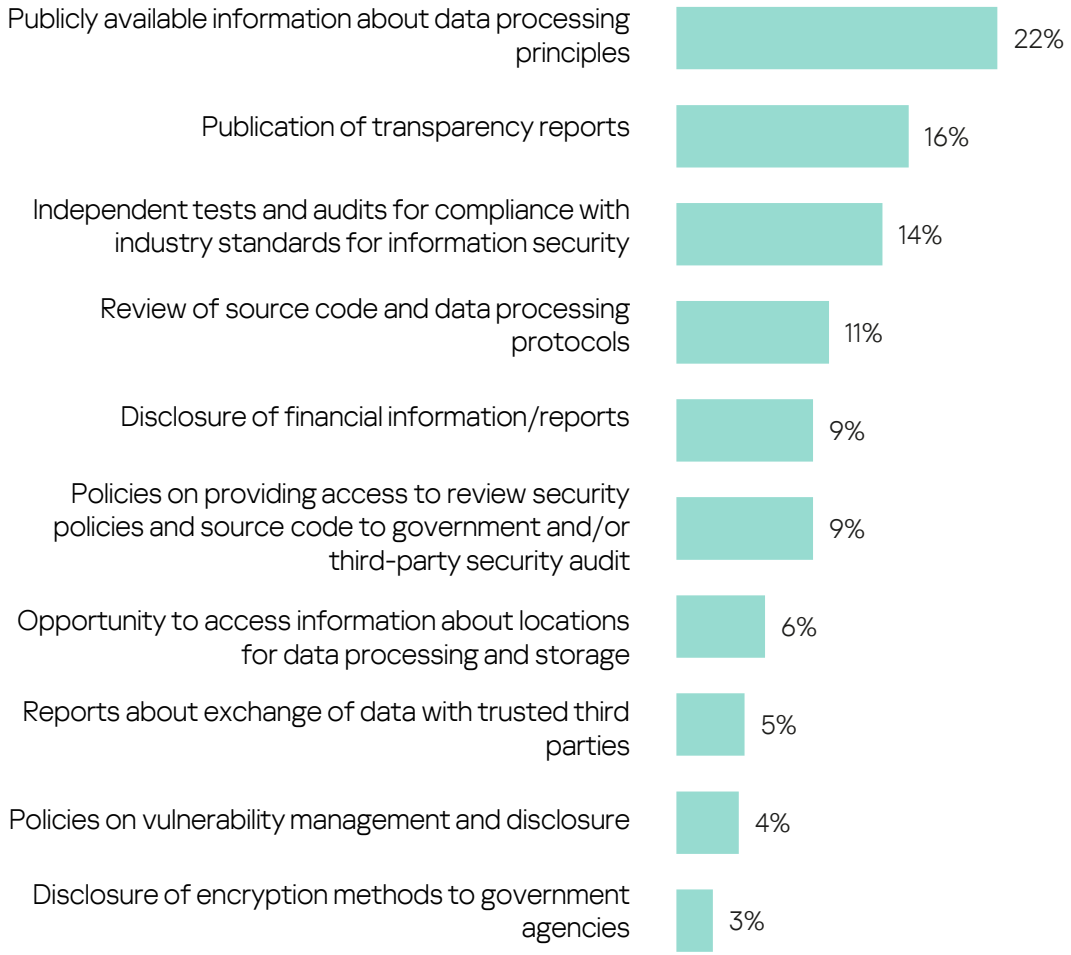
Learn more at the link.

Our research found almost 80 percent (78%) of worldwide surveyed respondents already have transparency policies in place within their organization. APAC businesses show the highest rate of transparency practice adoption — 88 percent, followed by North America (84%) and LATAM (82%). When it comes to transparency, these types of policy are more common for enterprises (82%), while 76 percent of SMBs have something in place.

Organizations also show willingness to invest resources in transparency development, with 81 percent revealing they are ready to allocate resources for the development of such policies. IT and telecoms companies and financial services sectors are most interested in such an investment, with 85 percent and 82 percent having stated their readiness.

When asked what these policies should include, the boundaries blur as no a clear definition or unanimity among organization could be shared.

The top three points listed by the majority of respondents included information about data processing principles (mentioned by 22%), publications of transparency reports (16%) and independent testing and audits for compliance with industry standards for information security (14%).




Practices and approaches covered by transparency policies

Proven.
Transparent.
Independent.

In 2017, Kaspersky launched its Global Transparency Initiative (GTI), which includes actionable and concrete measures to engage with the wider cybersecurity community and stakeholders in validating and verifying the trustworthiness of the company's products, internal processes and business operations. Learn more at the link.

# Data breaches affecting business

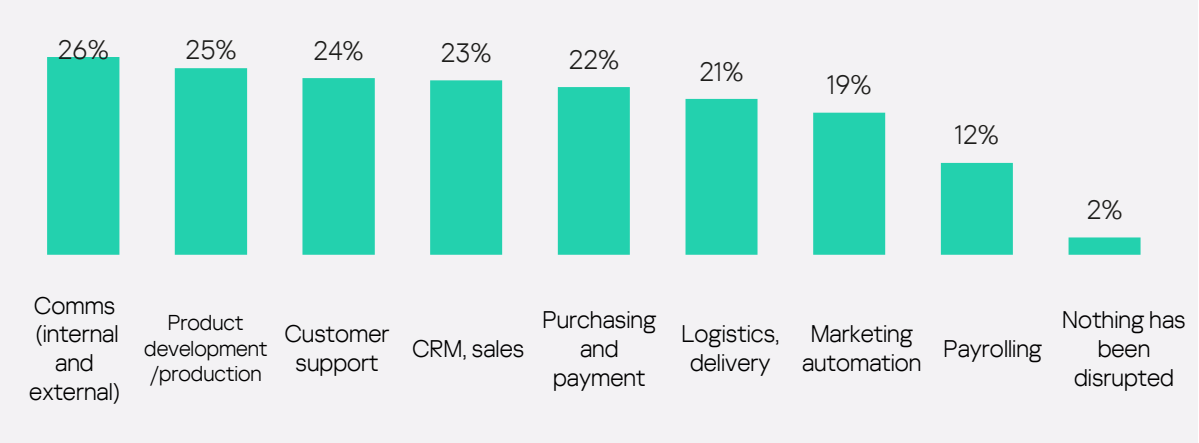
Most reported data breaches of internal systems caused either by cyberattacks (23%) or employees (22%) appear to be the most frequent security issue, while 20 percent of surveyed employees reveal identifying and remedying vulnerabilities in IT systems is the next biggest problem.

"Vulnerability management problems were reported by every fifth respondent and we're seeing our customers facing the same issues. The difficulty starts from the network inventory on the external resources when building the company's "digital footprint".

Enterprises and medium-size businesses have geographically distributed network resources with dozens of web-faced systems and applications using hosting providers and cloud services, requiring careful vulnerability management.

The problem is made worse by any new vulnerability or exploit as companies have no more than a few hours to apply any remediation measures before they will face multiple exploitation attempts from cybercriminals," says Yulia Novikova.

Cybersecurity breaches and intrusions affected communications (26%), product development and production (25%) followed by customer support (24%).

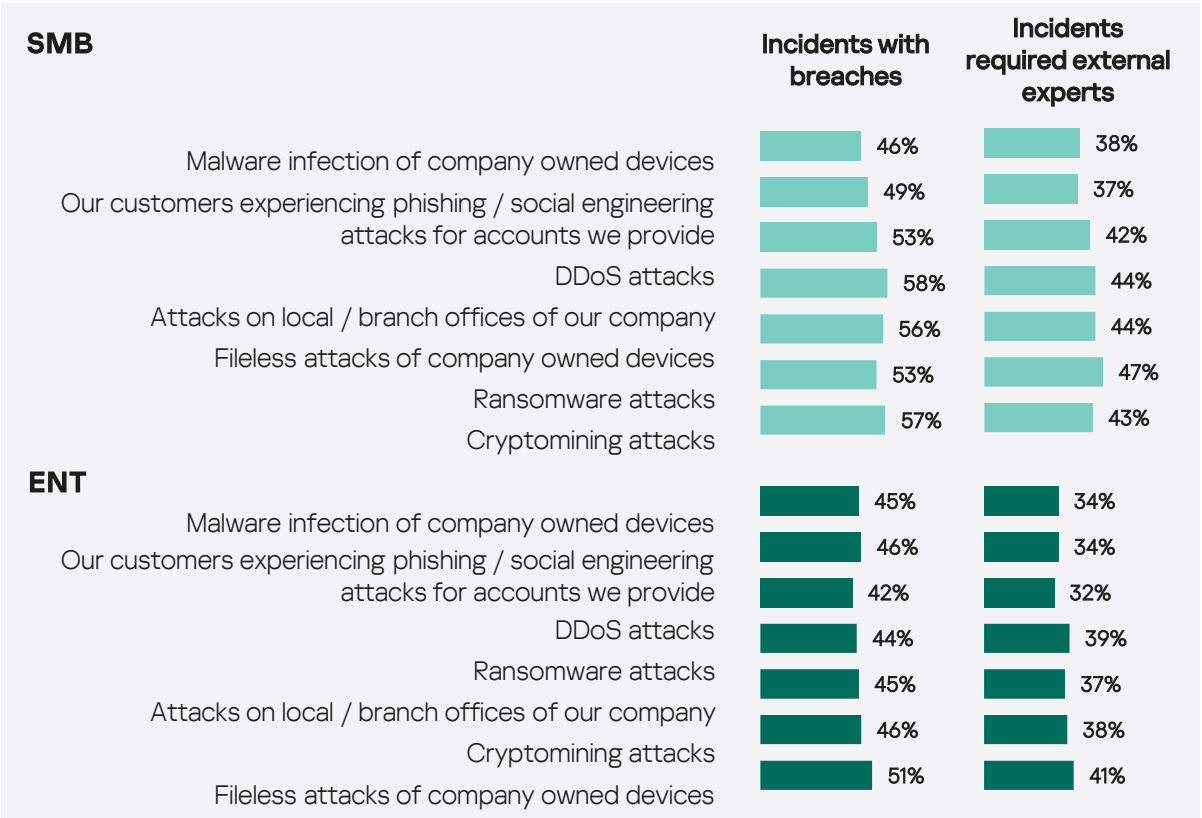


The most worrying data breaches affecting businesses of all sizes required additional costly expertise from external specialists in 2022.

Fileless attacks of company owned devices is one of the biggest challenge for IT security teams this year, with more than half of both SMBs (56%) and enterprise clients (51%) reporting intrusions.

Small to medium business respondents (58%) also mentioned attacks on branch offices and crypto mining (57%), while 46 percent of enterprise segment reported phishing and social engineering issues.

## Incidents with breaches & Participation of external experts: Business continuity



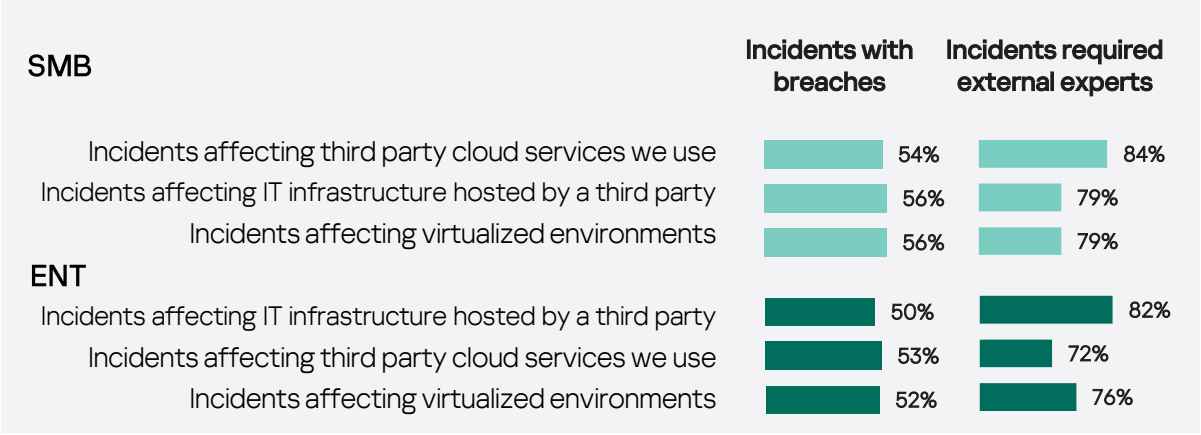

The top three incidents deemed complex enough to require external IT-security experts affected 76 percent of enterprise and 79 percent of SMB virtualized environments, IoT cloud services (72% ENT and 84% SMB) and IT infrastructure (82% ENT, 79% SMB).

Incidents involving the violation of IT security policies (30% ENT and 37% SMB) and inappropriate use of IT resources by employees (31% ENT and 36% SMB) required less external assistance.

Speaking of security issued of cloud infrastructure, in 2022, more than half of respondents said incidents affecting virtualized environments which involved an intrusion.

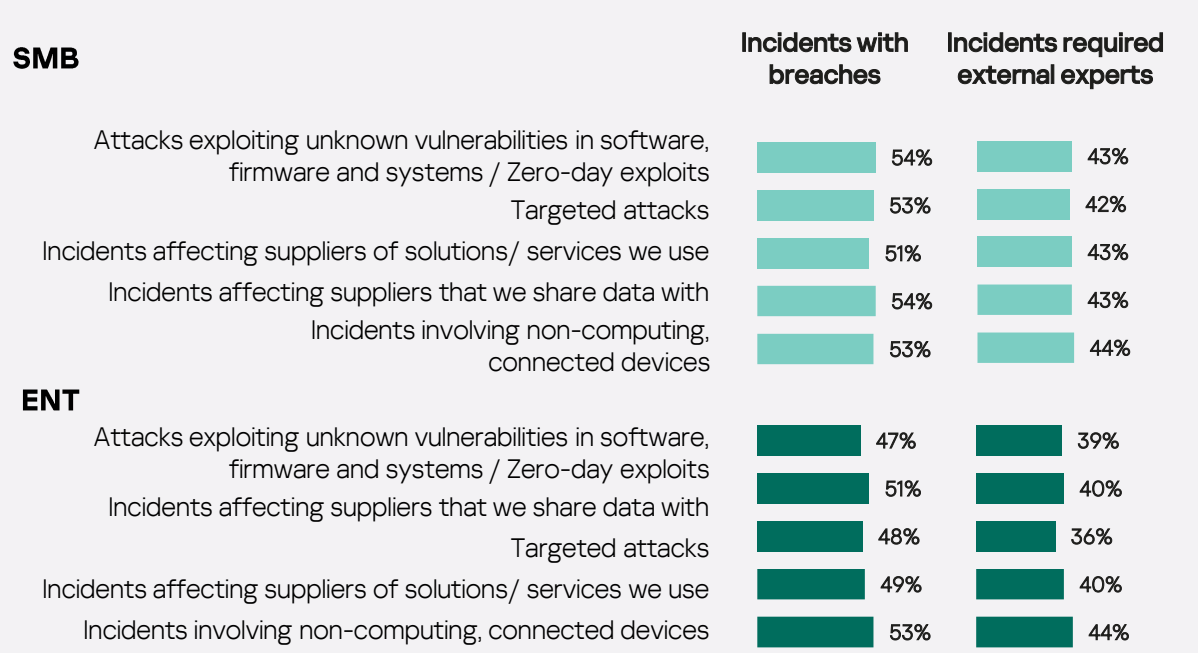
SMBs brought in external specialists to deal with third-party cloud service incidents (84%), while 82 percent of enterprise operations reported incidents with third party IT infrastructure.

## Incidents with breaches & Participation of external experts: Security issues of cloud infrastructure



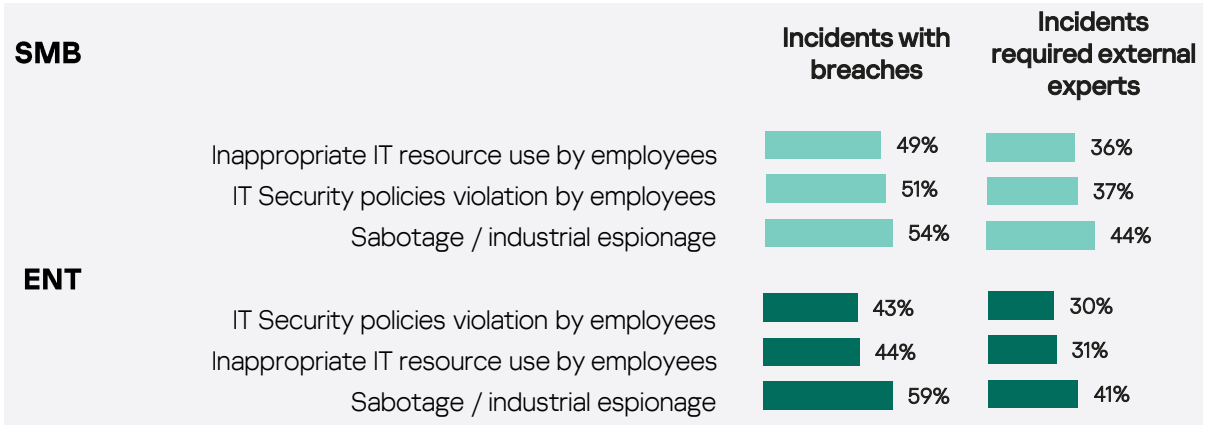

External IT professionals are increasingly being called to manage incidents involving non-computing and connected devices such as industrial control systems. The report reveals that such incidents have become a regular occurrence for 44 percent of enterprise respondents.

## Incidents with breaches & Participation of external experts: Securing complex environments



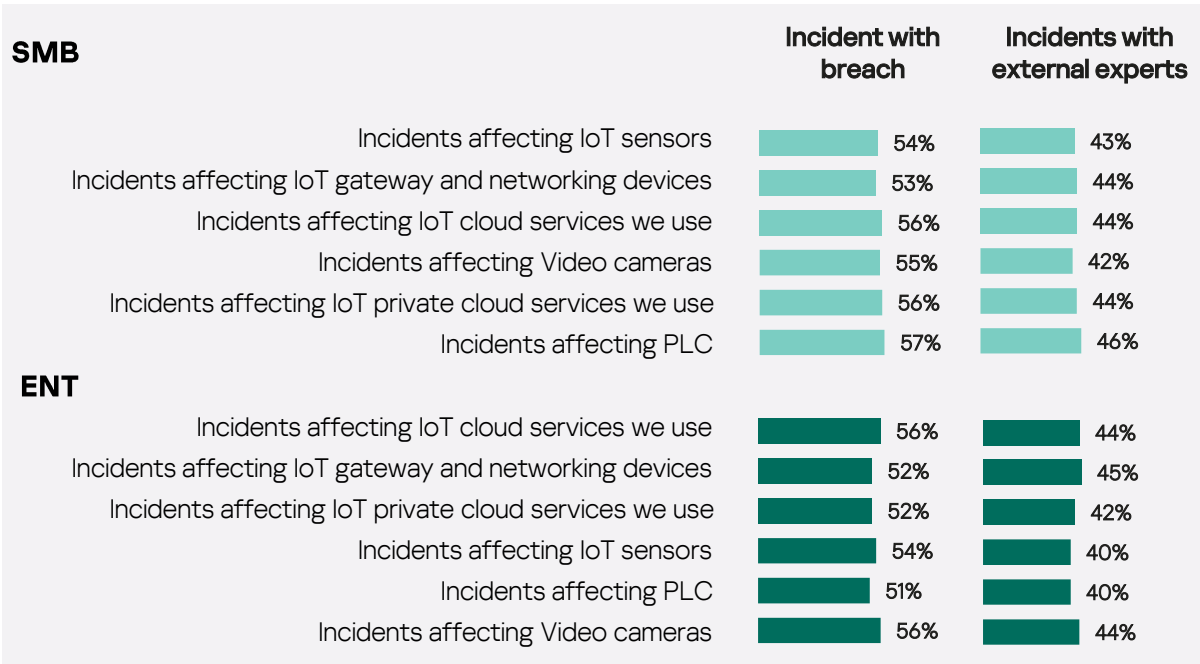
Large organizations unsurprisingly faced some form of sabotage or industrial espionage incidents (59% for enterprise, 54% for SMBs), requiring assistance from external experts.

## Incidents with breaches & Participation of external experts: Ensuring staff compliance




Assembly lines with robots and industrial computers with internet-enabled IoT programmable controllers to manage manufacturing processes are commonplace, but the most challenging security concerns for SMB now involve programmable logic controllers, PLC (57%) and IoT cloud services (56%), while the enterprise segment highlights most incidents affect cameras, IoT sensors and IoT cloud services as well (54-56%).

## Incidents with breaches & Participation of external experts: Security issues of IoT infrastructure



## The real-world cost of cyberattacks to business and enterprises

The average cost of recovery following a cyber-attacks is extremely high, but must be balanced with other financial demands on an organization.

Businesses need to prioritize capital expenditure on essential needs, such as recruitment or sales, while the high cost of a cyberattack will further increase budget burdens.

### ENT

**$109K**
The most expensive

**$53K**
The least expensive

- Targeted attacks and incidents affecting IoT private cloud services were the most expensive for the enterprise segment in 2022, costing **$104,488** and **$109,405** respectively.
- The least expensive incidents were caused by inappropriate use of IT resources by employees (**$52,887**).

### SMB

**$7.7K**
The most expensive

**$5K**
The least expensive

- For small-to-medium businesses, the most expensive attacks occurred on local or branch offices costing **$7,694**, while recoveries from DDoS attacks saw bills of **$7,298**.
- The less expensive incidents, those affecting suppliers, involved **$4,956** costs, while incidents caused by violations of IT security policies by employees required system repairs of **$4,951**.

## Additional dedicated cyber warriors

Recruitment is another priority on the list for IT security managers in 2023, who are looking to better protect their organizations from cyberthreats while also reducing response times. Additionally, after being exposed to a cyber incident, teams are also upskilling by adding dedicated specialist personnel with expert experience.

Overall, almost half of respondents (48%) invested in additional staff in 2022, to better respond to incidents that occurred. Recruiting additional IT security analysts or specialist staff in response to cyber security incidents was the best solution for 52 percent of SMBs and 56 percent of enterprises.

Half of SMBs and 46% of enterprises established new teams or people dedicated to IT security following a cyber incident. Additionally, 86% of companies have engaged with or employed IT professionals to address problems caused by incidents they have experienced over the last 12 months.

To expedite the situation, most companies have hired IT security consultants, with 57 percent of SMBs and 62 percent of enterprises employing outside services or consultants for cybersecurity risk assessments (32% for SMBs and 38% for Ent), or incident response cybersecurity services (28% SMBs and 33% Ent).

"From our experience, companies usually only start thinking about hiring dedicated information security professionals only after an incident has occurred, as information security is provided by a network administrator, programmer, or IT person. Also it's important to understand that one incident response specialist working without the right information security policies, relevant software, and hardware doesn't really have the capacity to deal with or be aware of every issue.

The best and most cost-effective way of reducing the cost of incidents is to be proactive and well-prepared for any possible cyberattack.

To protect and future-proof any business from malware infection or data breach, only by applying a full stack of proactive measures including an incident response plan creation, regular penetration testing, and information security audits can the cost of specialized personnel be justified.

In many cases the most economically feasible way to protect your business effectively – especially for small companies – is to engage with external professionals," comments Konstantin Sapronov, Head of Global Emergency Response Team at Kaspersky.

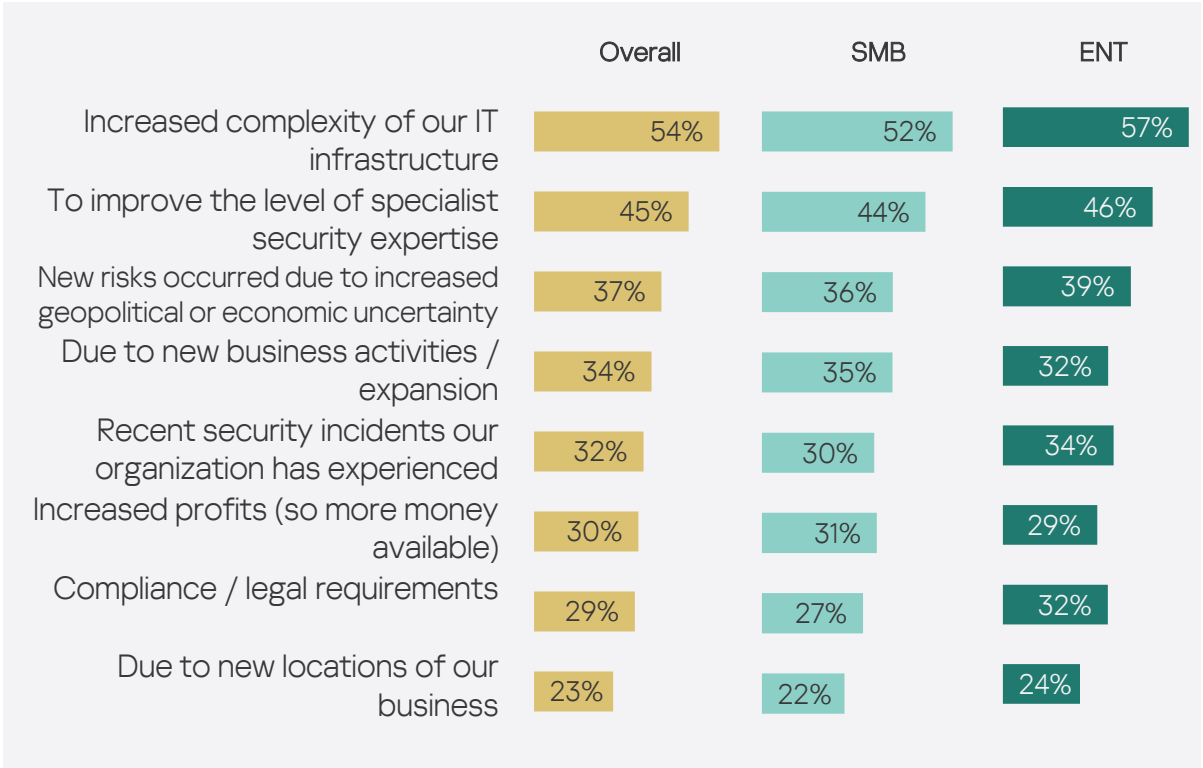
## Cybersecurity budgets to increase again in 2023

Cybersecurity budgets are set to increase again over the next three years for both SMBs and enterprises to cover a range of issues. In 2022, median enterprise IT budgets were US$12.5m and SMBs operated with $375,000 median IT budgets. Both SMBs and enterprises expect IT security budgets to grow by 14 percent over the next three years.

| | SMB Median | ENT Median |
|---|---|---|
| IT budget | $375,000 | $12,5M |
| IT Security budget | $150,000 | $3,75M |
| Expected average IT Security budget change over 3 year | +14% | +14% |

A top factor driving IT security budget increases were risks which occurred due to geopolitical or economic uncertainty for 36 percent of SMBs and 39 percent of enterprises.

## IT security budgets: Top factors driving spend



"Business continuity depends more than ever on information security, yet we still see large organizations operating either with unprotected systems, or with legacy equipment as they consider cyberattacks don't pose a threat to their business.

However, as IT Infrastructure is now increasingly complex and cyberattacks are more sophisticated, such businesses are becoming more cyber-aware as they need to protect every asset inside the organization, including computers, data, users and to expand cyber defense to the limit of all possible attack vectors.

Some states now require organizations to be more cyber and data secure, and whether it's a regulator requiring a designated person for this role, or new rules for an entire vertical or industry, these are factors influencing growing budgets," comments Ivan Vassunov, VP, Corporate Products at Kaspersky.

## Changing business needs resolved with MSP solutions

With rapidly changing business needs and priorities in 2022, many companies outsourced certain IT functions to managed service providers (MSP) and managed security service providers (MSSP) when looking to make budget efficiencies or up skill teams.

The number one reason to outsource certain IT security responsibilities to MSP/MSSP in 2022 was to drive efficiencies in the delivering cybersecurity solutions both for SMBs (62%) and enterprise (69%). Among other most frequently mentioned reasons for outsourcing included a shortage of IT employees or understaffing in IT departments (53% for SMBs) and a requirements of special expertise (50% for SMBs and 52% enterprise). Additionally, 47 percent of enterprises have sourced outside experts to manage complex business processes for their organization.

# Conclusion

Another testing year for IT teams working with less staff reveals that the cyber-threat landscape continues to be challenging, with attacks on business persisting. But with increasing IT spend on the horizon, future management of security incidents and breaches look positive as businesses are taking a more proactive stance on cybersecurity.

While malware infections and phishing attacks remain the top threats, the new data leaks were from within the organization - mainly caused by employees – are an additional headache for IT security teams transitioning certain functions to outsourced services.

After two years of cost-saving measures, businesses large and small are now moving into a post-pandemic world and adapting to life with cloud-based IT due to increased complexity of IT infrastructure.

Protecting organizations across remote and cloud IT infrastructure during the pandemic may not be the panacea, but in the current economic and geo-political environment, it offers some peace of mind when meeting ever-changing corporate security requirements.

To face the ongoing threats of malware and phishing, and to protect your businesses from unwanted data breaches and information leaks, Kaspersky recommends the following:

Anticipate and budget cyber and data risks relevant to your country and industry by using specialized resources such as IT Security Calculator. This tool will help you to maximize the efficiency of your protective measures.

Use a multi-platform adaptive security solution such as Kaspersky Endpoint Detection and Response (EDR) to provide comprehensive visibility across all endpoints of a corporate network, allowing automation of routine EDR tasks and enabling cyber teams to speedily hunt, prioritize, investigate and neutralize complex threats.

Additional expertise without additional hiring can be achieved by adopting a managed security service such as our Managed Detection and Response (MDR). It allows the best possible advanced automated security services and analysis of corporate data gathered every day, in real time, 24/7, to help protect against sophisticated cyberattacks, even if company lacks security workers.

Invest in training your IT security specialists, keep their skills up-to-date and are best prepared for the cyber threat landscape. With Kaspersky Expert training, InfoSec professionals can advance their skills or assist team managers help incident response teams battle today's evolving cyber-reality.

Think in advance where you can apply for help in case a cybersecurity incident happens. While it is not always possible to halt an attack before it penetrates your security perimeter, a professional aid from security experts can help to limit the resulting damage and prevent the attack from spreading.