Digital Security
Progress. Protected.

ESET SMB Cybersecurity Report 2024

CYBERSECURITY™
MADE IN EUROPE

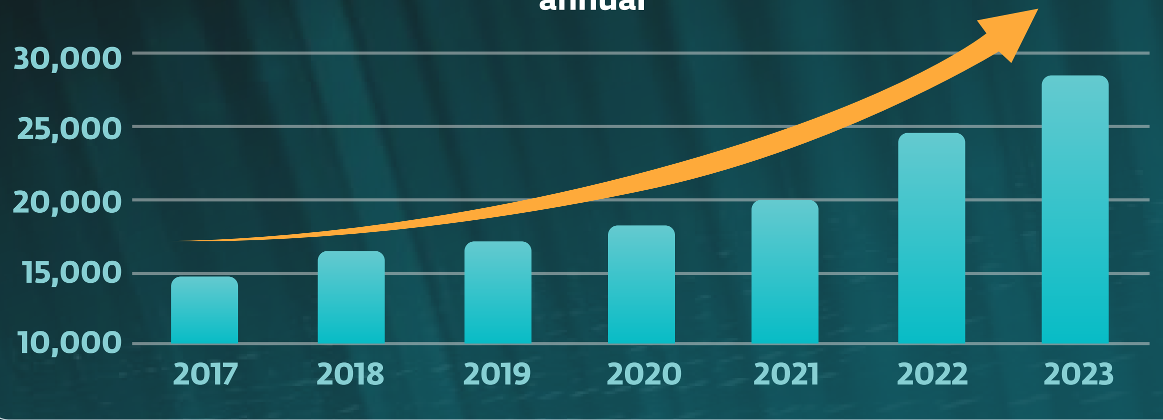
2023
Record surge in unseen malware and software vulnerabilities

Two **key indicators** suggest that data breaches and cyberattacks will become increasingly common in the near future.

Cybercriminals deployed a record number of new malware, with ESET detecting over **500,000 unique malware daily** on average.

Secondly, **the number of software vulnerabilities, including operating systems, hit a record high last year** for the seventh time in a row, with an average of 80 new vulnerabilities daily.

Number of Common Vulnerabilities Exposures (CVEs) published, annual



500,000

New, unique malware detected daily

DID YOU KNOW?

An **exploit** leverages vulnerabilities in software to compromise a computer system, often for malicious purposes. This can involve installing malware such as ransomware or spyware, or stealing sensitive data, among other harmful activities.

Foreword

"Cybercriminals are orchestrating increasingly sophisticated attacks on organisations with unprecedented precision. **Small and Medium-sized Businesses (SMBs) are not exempt from these threats**; in fact, they are often the prime targets due to their perceived vulnerability.

However, the narrative here is not one of fear, but of empowerment. Effective cybersecurity models, such as **Singapore's Cyber Essentials Mark and Australia's Essential Eight**, offer valuable frameworks for SMBs. By leveraging these models and other tools, SMBs can enhance their defences and thrive in the face of adversity.

Ultimately, **proactive defense remains the best cybersecurity strategy. "**

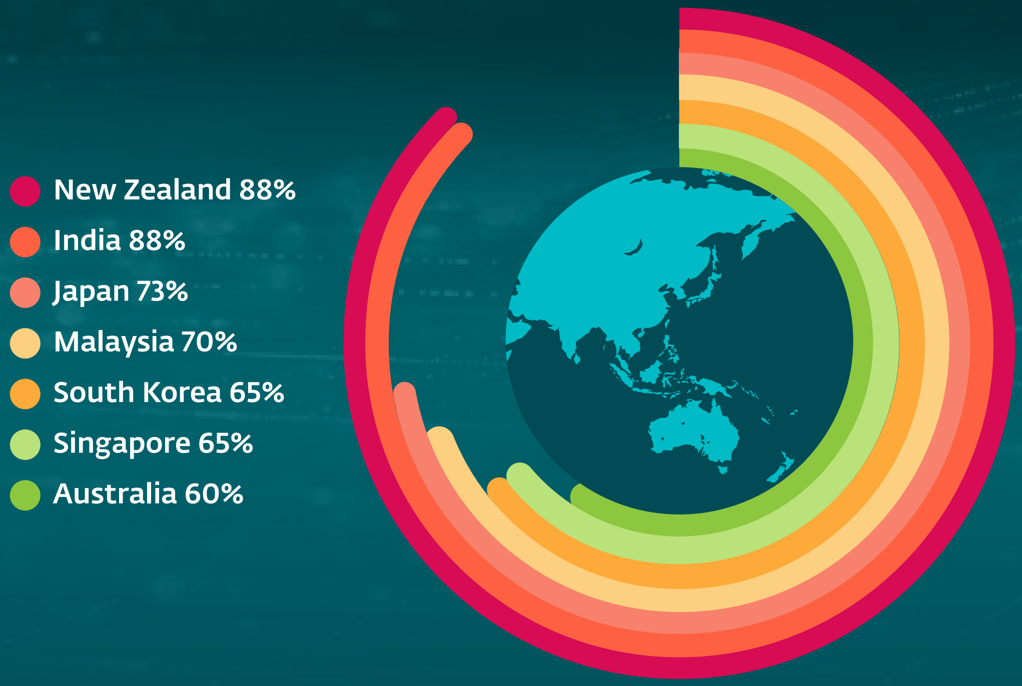
PARVINDER WALIA
PRESIDENT OF ASIA PACIFIC & JAPAN (APJ) ESET

Cybersecurity incidents affecting SMBs are incredibly common

7 out of 10

organisations surveyed across APAC have experienced a cybersecurity breach or acted on strong indications of a data security incident in the past year.

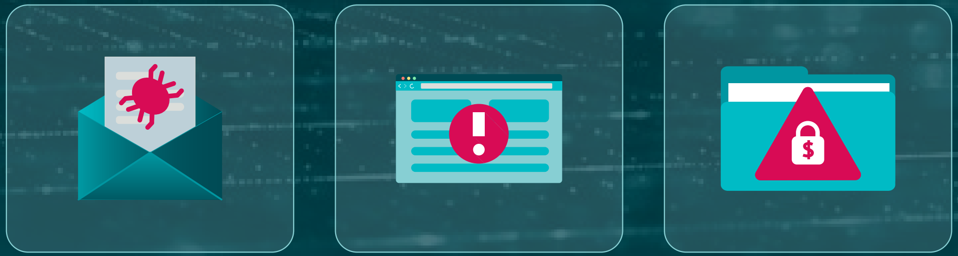
India and New Zealand reporting a significantly higher incidence rate, at 88%.



Majority of SMBs said they experienced cybersecurity incidents in the last 12 months

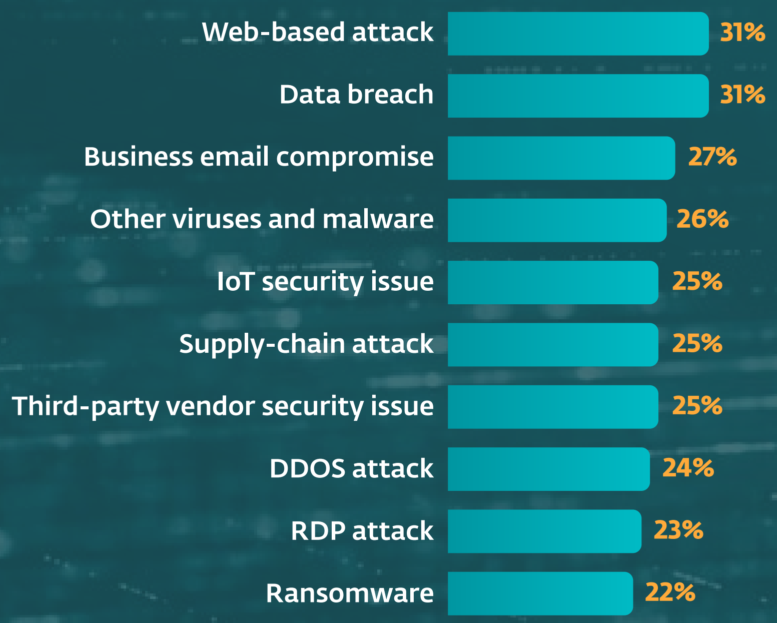
Web-based attacks and data breaches topped the list

Web-based attacks and data breaches were the most prevalent cybersecurity breaches or incidents with 31% incidence rate.



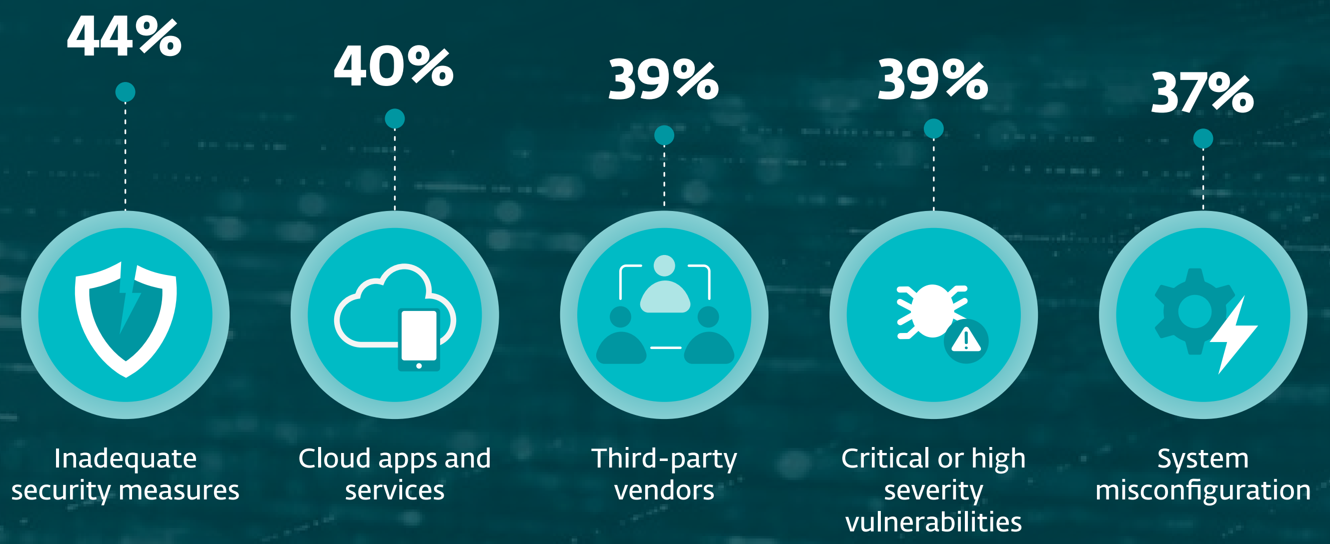
India saw significantly higher of web-based attacks at 42% compared to other countries.

Singapore reported more business email compromises at 34%, and Malaysia reported higher ransomware attacks at 31%.



What are the major factors that led to cybersecurity breaches or incidents?

44% of SMBs cited a lack of adequate defences, exposing their organisations to breaches or cybersecurity incidents. Third-party vendors, and the presence of critical or high severity vulnerabilities also added to the risk.



44%

Inadequate security measures

40%

Cloud apps and services

39%

Third-party vendors

39%

Critical or high severity vulnerabilities

37%

System misconfiguration

Main contributing causes for cybersecurity incidents

Did you know?

Cloud-based email, collaboration and storage apps commonly used by SMBs are also susceptible to threats, including ransomware. It is crucial for businesses to add an additional layer of protection for such cloud apps to prevent cyberattacks in their network.

Universal fears

Amidst the cyber landscape, viruses and malware, web-based attacks, business email compromise, ransomware and AI-enhanced threats stand as the **foremost concerns** for SMBs in the next 12 months.

VIRUSES AND MALWARE	WEB-BASED ATTACKS	BUSINESS EMAIL COMPROMISE	RANSOMWARE	AI-ENHANCED THREATS
81%	78%	78%	77%	77%

Top 5 cybersecurity threat concerns in APAC

Did you know?

Email is the no.1 threat vector as it can be easily used to deliver malware, harmful script and phishing scams.

In business email compromise (BEC) attack, the most common goal is to convince the target to send money to the attacker while believing that they are performing a legitimate, authorised business transaction. This usually involves impersonation and the use of a seemingly legitimate email address or phone number the victim is familiar with.

Most SMBs would consider paying ransomware demand

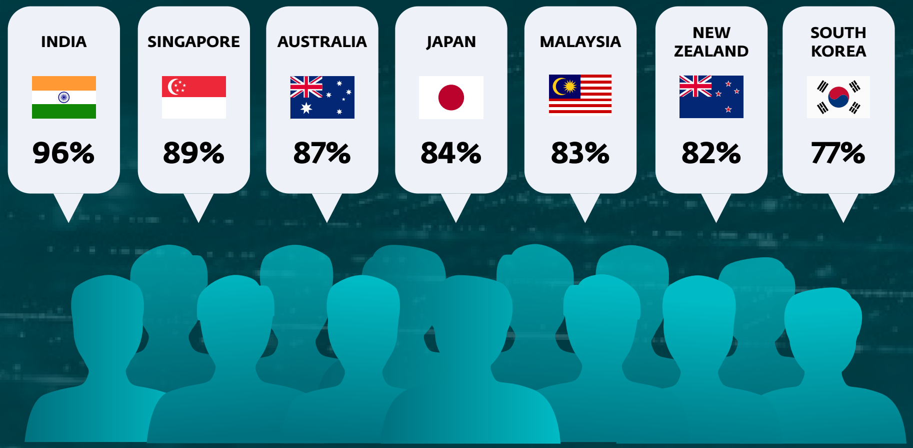
86%

would consider making payments to cybercriminals in the event of a successful ransomware attack.

This is despite the fact that many authorities worldwide do not recommend paying ransom as there's no guarantee that the victim will receive the decryption key or their stolen data will not be published.

22% of respondents experienced cybersecurity incidents related to ransomware in the past 12 months.

Majority said they would consider paying ransomware in the event of a successful attack



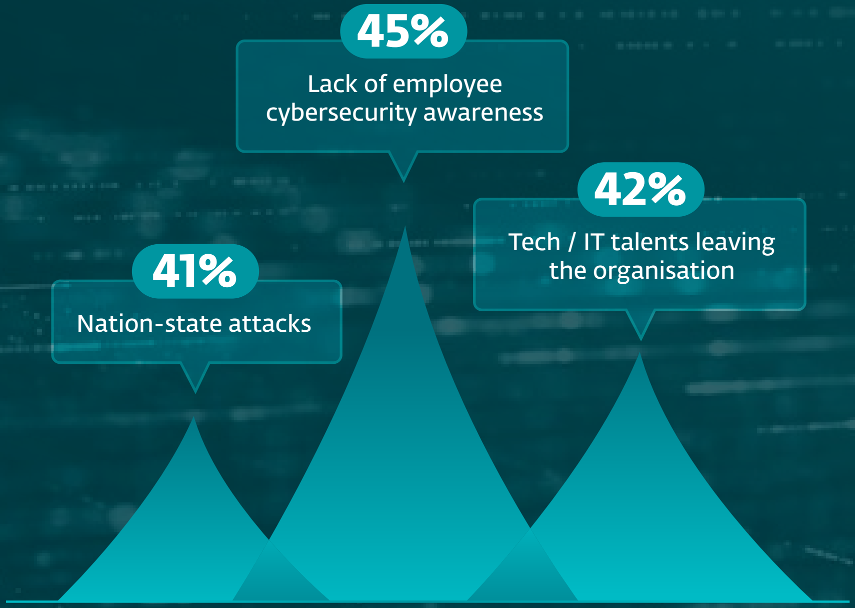
Did you know?

A recent report suggested a total of US$1.1 billion was extorted from victims of ransomware in 2023*. Ransomware has become such a lucrative business model that operators offer Ransomware-as-a-Service (RaaS) to other cybercriminal groups, further fuelling the increase in ransomware attacks.

[1] *Source: https://www.businesstimes.com.sg/companies-markets/banking-finance/crypto-ransom-attack-payments-hit-record-us1-billion-2023*

Organisations need to prioritise awareness

A **deficiency in employee cyber awareness** ranks among the top factors that respondents think will impact the risk of cyberattacks in the upcoming 12 months.



Top factors impacting risk of cyberattacks

The risk battleground is diverse

Respondents from different countries rank the following factors as the greatest impact to cybersecurity in the next 12 months.

Top factors impacting risk of cyberattacks

	OVERALL	JP	AU	IN	SG	MY	SK	NZ
Lack of employee cyber awareness	**45%**	34%	50%	50%	49%	51%	37%	44%
IT talent leaving the organisation	**42%**	35%	36%	45%	46%	44%	38%	50%
Nation-state attacks	**41%**	41%	39%	50%	40%	46%	35%	41%
Vulnerabilities in the supplier ecosystem	**39%**	36%	39%	39%	36%	49%	26%	46%
Increase of multiple apps by employees	**38%**	35%	38%	44%	48%	41%	30%	38%
Use of remote desktop protocol	**36%**	33%	35%	41%	43%	36%	31%	35%
Generative AI	**36%**	28%	33%	40%	43%	44%	28%	38%
Increase use of cloud productivity suites	**35%**	32%	37%	38%	36%	34%	29%	37%
Continued hybrid or home working	**34%**	34%	35%	39%	33%	34%	23%	41%

What are the top cybersecurity challenges?

Overall, respondents ranked **lack of a dedicated cybersecurity team, alert fatigue and keeping up with the latest threats** as the top 3 challenges.

When we take a closer look, the top 2 challenges are significantly higher than the rest – 27% for lack of a dedicated cybersecurity team and 26% for alert fatigue.

Lack of a dedicated cybersecurity team is the top challenge in Japan, Australia, Malaysia, South Korea and New Zealand, while SMBs in India and Singapore said alert fatigue.

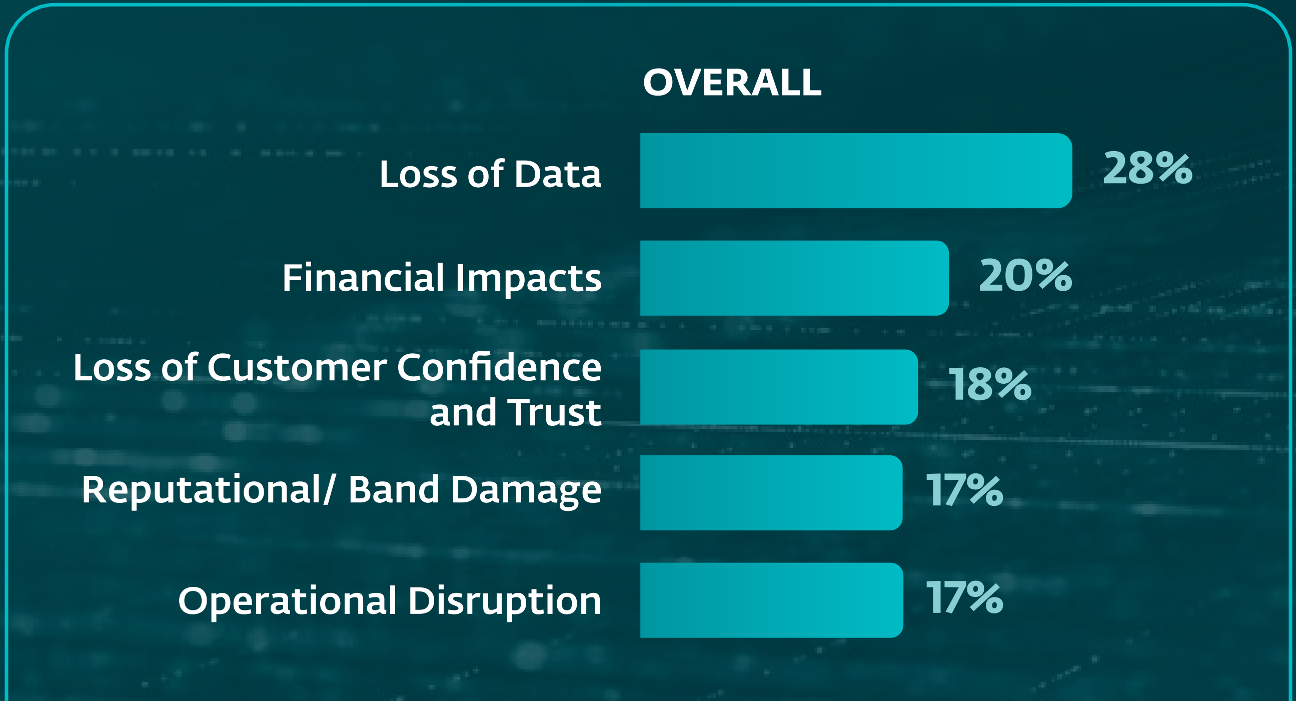
Top cybersecurity challenges faced by SMBs

	OVERALL	JP	AU	IN	SG	MY	SK	NZ
No dedicated cybersecurity team	27%	30%	29%	23%	23%	25%	32%	29%
Alert fatigue	26%	26%	26%	36%	31%	24%	23%	20%
Keeping up with the latest threats	14%	8%	13%	15%	16%	17%	13%	17%
Understaffed and overworked IT team	14%	14%	13%	9%	17%	13%	17%	15%
No support from the leadership	8%	12%	12%	7%	5%	8%	7%	8%
Keeping up with the latest technologies	7%	7%	6%	10%	5%	8%	6%	10%
Buddget limitations	3%	4%	3%	2%	5%	7%	4%	2%

Did you know?

High false positives or a poorly configured security solution can overwhelm IT administrators with too many security alerts. This may lead to desensitisation, causing them to ignore real threat alerts.

Cybercriminals’ success is SMBs’ loss



SMBs’ biggest business implication concerns in the event of a successful cyberattack

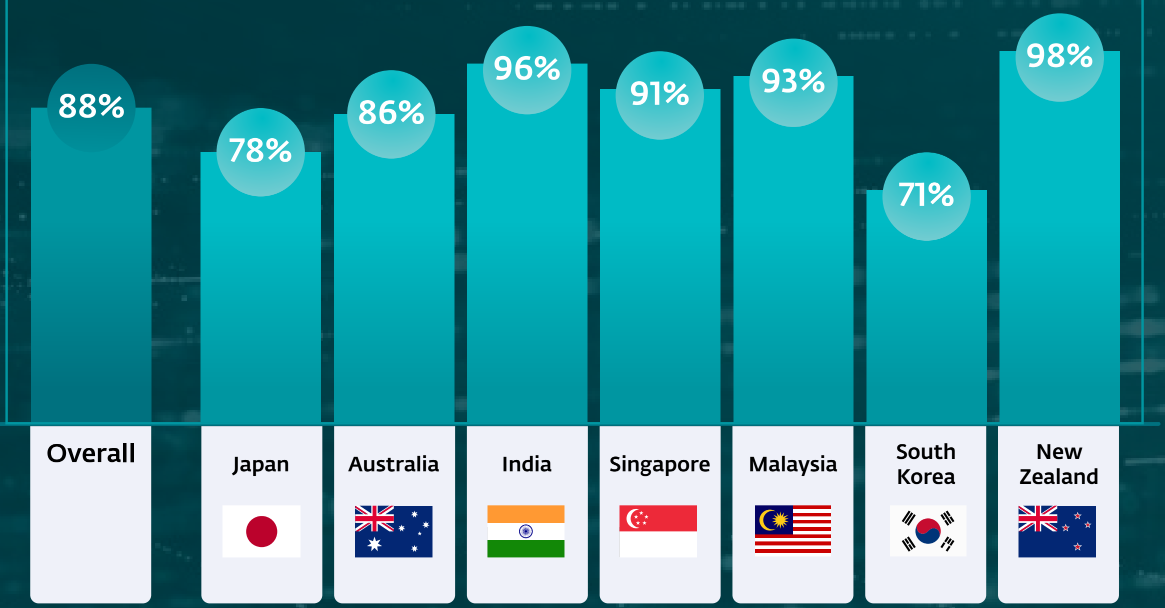
The road ahead is paved with confidence, or is it?

Despite almost **9 out of 10 SMBs expressed confidence in their cyber resilience over the next 12 months**—particularly respondents in India, Malaysia, and New Zealand—44% of those affected by cybersecurity incidents cited inadequate security measures as the primary contributing factor.

82%

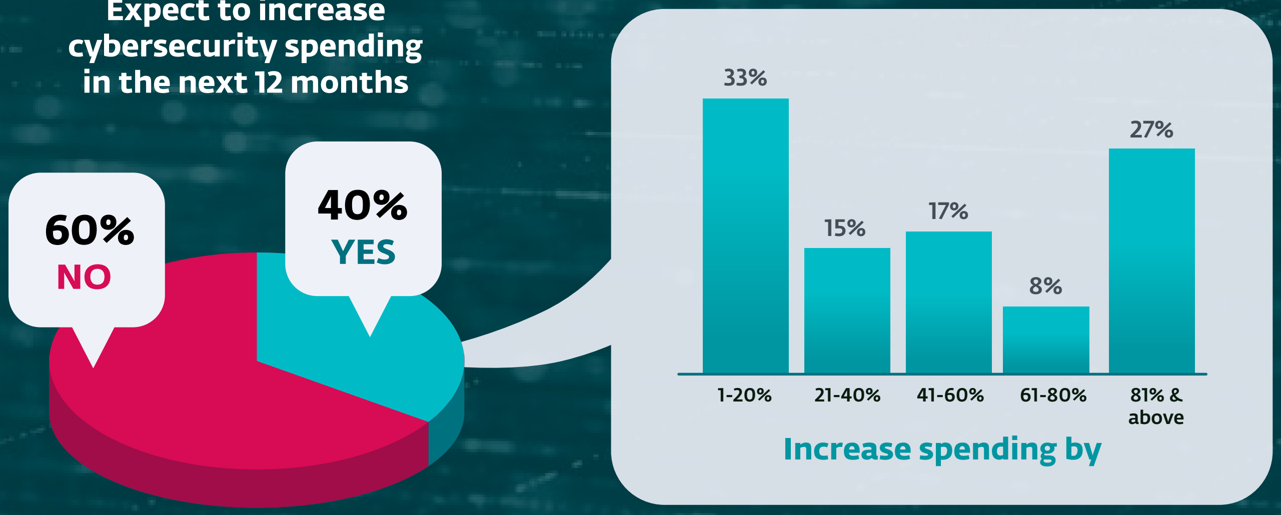
agreed that SMBs are more vulnerable to cyberattacks compact to larger enterprises

Most SMBs said they are confident in their cyber resilience



SMBs are increasing their spending in cybersecurity

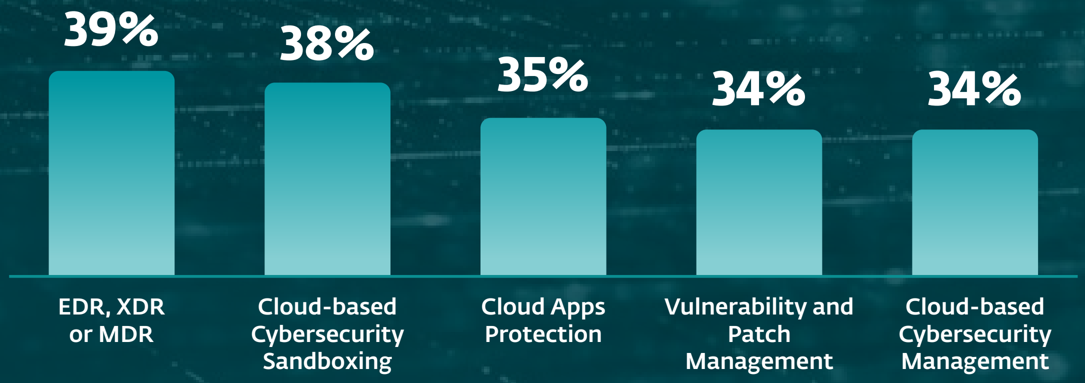
To bolster their resilience and protection measures, **4 out of 10 respondents anticipate an increase in cybersecurity spending over the next 12 months**, with over 35% expecting substantial increase of over 60% in spending.



Most SMBs said they are confident in their cyber resilience

Acquiring more protection: Leave no stone unturned

SMBs aimed to boost resilience with solutions that they are not currently using such as EDR/XDR/MDR, cloud-based cybersecurity management, vulnerability and patch management, and cloud-based sandboxing.



Did you know?

Cloud-based cybersecurity sandbox is one of the important tools to analyse unknown, never-before-seen type of threats including ransomware.

It provides powerful, isolated test environment in which suspicious programs can be executed, and their behavior observed, analyzed and reported in an automated manner within minutes.

SMBs ramp up cybersecurity post-incident, but prevention is the best strategy

More than half of the SMBs surveyed conducted risk audits and invested in more cybersecurity training to bolster their cybersecurity posture following a cybersecurity breach or incident.

	OVERALL	JP	AU	IN	SG	MY	SK	NZ
Conducted a cybersecurity risk audit	51%	37%	43%	55%	56%	52%	54%	55%
Invested in more cybersecurity training	50%	41%	47%	57%	51%	59%	42%	50%
Invested in new cybersecurity tools	49%	40%	44%	57%	51%	58%	42%	49%

Prevent data breaches with an effective cybersecurity strategy

In the face of limited resources, SMBs are challenged to achieve more with less. Hence, it is crucial for them to prioritise investment in prevention, effectively minimizing cyber risks before they evolve into serious threats.

Utilize multilayered endpoint security software supported by artificial intelligence, human expertise, and cloud-based sandboxing to defend against advanced threats, including new and previously unseen threats, as well as ransomware.

Ensure that all endpoints are encrypted to prevent data loss.
Merely locking devices with a password is insufficient, as criminals can still access the data by removing the hard drive.

Implement multifactor authentication (MFA) and maintain regular updates.
Data breaches commonly result from username and password theft.

Use a vulnerability and patch management solution to ensure software vulnerabilities are timely patched, as out-of-date software and operating systems can be exploited by cybercriminals. These can lead to malware infections, unauthorized control of your devices, or even data theft.

Provide cybersecurity training for employees because individuals who can identify phishing attempts, avoid online scams, and adhere to internet best practices add a crucial layer of protection to prevent breaches.

About the study

SURVEYED MARKETS

Japan

Australia

India

Singapore

Malaysia

South Korea

New Zealand

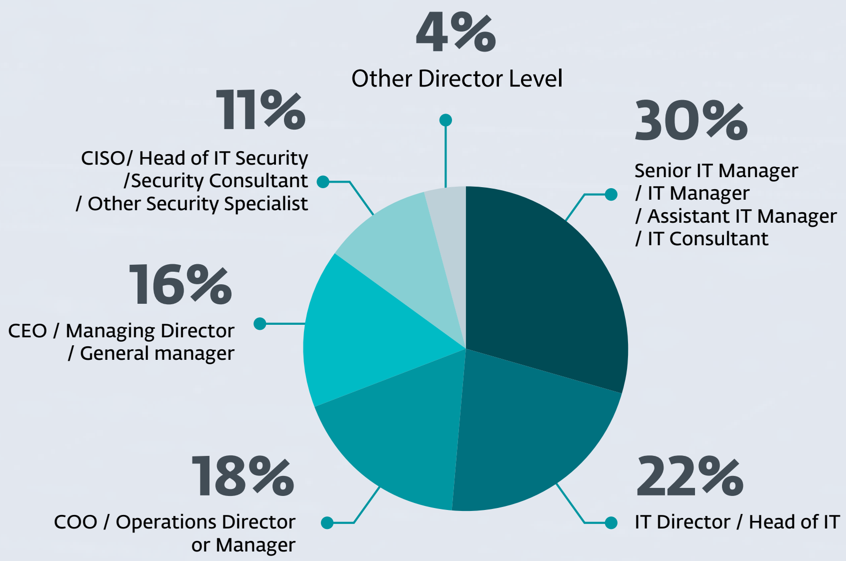
SURVEYED SIZE

Total 1,400 respondents

RESPONDENTS' PROFILES:

IT decision makers from organisations of various verticals with between 25 to 200 employees.

RESPONDENT'S JOB ROLES:



Study conducted in partnership with Blackbox Research.

ESET helps SMBs achieve Essential Eight

In the face of limited resources, SMBs are challenged to achieve more with less. Hence, it is crucial for them to prioritise investment in prevention, effectively minimizing cyber risks before they evolve into serious threats.

	ESET PROTECT All packages	ESET PROTECT Complete	ESET PROTECT Enterprise	ESET PROTECT Elite	ESET PROTECT Elite + ESET Secure Authentication
Configure Microsoft Office macro settings	✓	✓	✓	✓	✓
User Application Hardening	✓	✓	✓	✓	✓
Patch Operating Systems	✓	✓	✓	✓	✓
Patch Applications		✓	✓	✓	✓
Application Control			✓	✓	✓
Multi-factor Authentication					✓
Restrict Administrative Privileges	Support available through our partner network				
Regular Backups	Support available through our partner network				

*Through ESET Technology Alliance partner

ESET PROTECT COMPLETE

Multi-vector protection reducing attack surface

Complete protection for endpoints, cloud applications and email, the #1 threat vector. Cross-platform solution with cloud management, server security, advanced threat defense, encryption and vulnerability patching.

★★★★★

> **“It’s nice to know that our endpoints are now secure, and we can go hard and early on potential threats.”**
>
> Bob Kambora, IT Manager

INCLUDED MODULES

Console

Server Security

Modern Endpoint Protection

Mobile Threat Defense

Advanced Threat Defense

Full Disk Encryption

Cloud Application Protection

Provides advanced protection for cloud email, collaboration and storage against malware, spam or phishing attacks with ultimate zero-day threat defense and an easy-to-use console.

- An additional layer of protection for Microsoft 365 and Google Workspace apps (Exchange Online, OneDrive, Teams, SharePoint Online, Gmail and Google Drive)
- Automatic protection of new users
- Immediate notification when malware is detected

Mail Server Security

Additional layer of defense to prevent spam and malware from ever reaching users’ mailboxes.

- Robust quarantine management
- Multilayered technology filtering spam and malware
- Anti-phishing protection

Vulnerability & Patch Management

Actively tracks vulnerabilities in operating systems and common applications and enables automated patching across all endpoints.

- Severity-based prioritization of vulnerabilities
- Wide range of filtering options
- Automatic and manual patching options

Industry-leading technology from ESET

AI-native, multilayered approach to digital security

Our proprietary technology, ESET LiveSense, features several layers of protection. It works alongside ESET LiveGrid, our cloud-powered threat hunting technology, which collects and analyzes a vast array of suspicious samples. Combined with AI and our human expertise, ESET's security solutions offer real-time protection against ever-evolving cyber threats.

ESET LiveGrid®

Whenever a zero-day threat such as ransomware is seen, the file is sent to our cloud-based malware protection system, ESET LiveGrid®, where the threat is detonated and behavior is monitored. Results from this system are provided to all endpoints globally within minutes, without requiring any updates.

Artificial Intelligence

Uses the combined power of neural networks and handpicked algorithms to correctly label incoming samples as clean, potentially unwanted or malicious. To offer the best detection rates and lowest possible number of false positives, ESET Augur, our machine-learning engine, is fine tuned to cooperate with other protective technologies such as DNA, sandbox and memory analysis, to extract behavioral features.

Human Expertise

It's not all about technology. ESET invests heavily in its people to ensure we have an educated and trained workforce that wants to stay with the company. World-class security researchers share their knowledge to ensure the best round-the-clock global threat intelligence.

THIS IS ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats with our prevention-first approach, powered by AI and human expertise. Experience best-in-class protection thanks to our in-house global threat intelligence, refined for over 30 years, fueling an extensive R&D network led by industry-acclaimed researchers.

ESET protects your business so you can unlock the full potential of technology.

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS Drive your Ambition	Allianz Suisse	Canon Canon Marketing Japan Group	T · ·
protected by ESET since 2017 more than 9,000 endpoints	protected by ESET since 2016 more than 4,000 mailboxes	protected by ESET since 2016 more than 32,000 endpoints	ISP security partner since 2008 2 million customer base

SECURITY CERTIFIED

ISO security certified

ESET is compliant with ISO/IEC 27001:2013, an internationally recognized security standard in implementing and managing information security.

OPSWAT certification

ESET boasts Platinum OPSWAT Access Control Certification for Endpoint Security Applications.

Cybersecurity Made In Europe

ESET is one of the first IT security companies to be awarded the "Cybersecurity Made in Europe" label by the European Cyber Security Organization (ECSO).

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

200
countries and territories

13
global R&D centers

Digital Security
Progress. Protected.