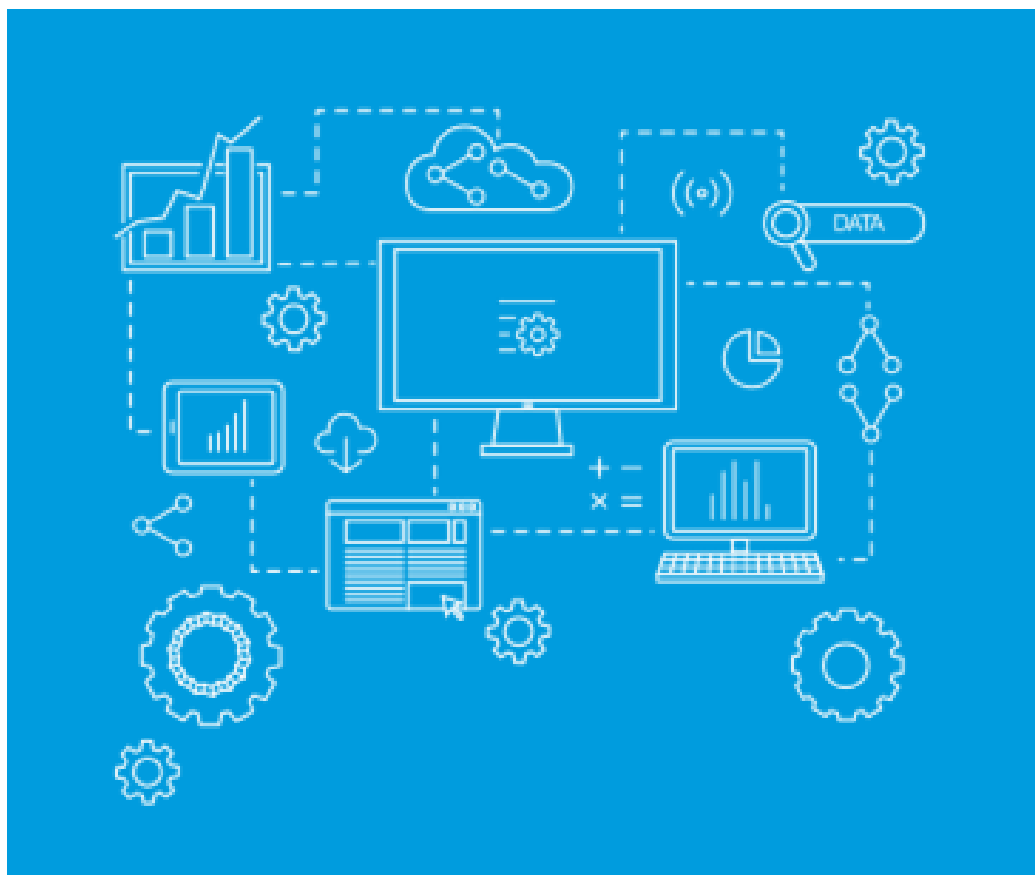


EMERGING THREATS IN CYBERSECURITY

RSM INDONESIA SPECIAL REPORT



THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING



Table of Contents

EXECUTIVE SUMMARY	2
SURVEY HIGHLIGHTS.....	3
RESPONDENTS	4
RESPONDENT DEMOGRAPHIC	4
INFORMATION SECURITY AND DATA PROTECTION	6
CYBERSECURITY AWARENESS FOR VIRTUAL INTERACTION TRENDS.....	6
INFORMATION SECURITY AND DATA PROTECTION GOVERNANCE.....	6
INSIGHTS FROM RSM INDONESIA.....	7
CYBERATTACKS AND THREATS	8
EXPERIENCED A CYBERATTACKS.....	8
IMPACT OF CYBERATTACKS.....	9
REPORTING AND FOLLOW-UP ON CYBERATTACKS	9
ACTIONS ORGANIZATION HAS TAKEN TO ADDRESS CYBERSECURITY THREATS.....	10
INSIGHTS FROM RSM INDONESIA.....	11
CYBER INSURANCE	12
THE BENEFIT OF CYBER INSURANCE	12
ORGANIZATION CARRIES A CYBER INSURANCE POLICY	12
RISKS AND EXPOSURES OF CYBER INSURANCE	13
INSIGHTS FROM RSM INDONESIA.....	14
THE REASONS WHY ORGANIZATIONS MOVE OR MIGRATE DATA TO THE CLOUD	15
INSIGHTS FROM RSM INDONESIA.....	16
CONCLUSION AND RECOMMENDATION	17

EXECUTIVE SUMMARY

The unprecedented and large-scale shift of employees to remote work in response to global quarantines and lockdowns is the most prominent driver of increased risk. Accommodating a remote workforce quickly requires great attention to operational and security considerations¹. Most organizations were unprepared for sudden change, and those that are not positioned to move quickly to a remote or largely remote workforce struggle to adapt.

Providing the appropriate IT infrastructure and assets, such as network support and laptops, to work from home on short notice creates challenges for IT teams. Challenges range from slow adoption to relying on outdated systems, both increasing the risk of disrupted operations and successful cyberattacks.

Rapid implementation of remote working models enhances cyberattacks by exacerbating existing technology vulnerabilities. It also reduces the organization's visibility into employee behaviour and the increasing number of devices now connected to the organization's network, puts a strain on IT operations and security professionals.

Cybersecurity, regardless of the pandemic, has also been on the top for three years in a row, as rated by OnRisk. The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.²

On the other hand, hackers and other electronic criminals continued their relentless pursuit of data and sensitive information from middle market businesses, leading to record levels of several types of attacks. The middle market continues to represent a sweet spot for hackers, with organizations possessing a significant amount of valuable data, but lacking the level of protective controls and staffing of larger organizations.

In this report, we explore respondents' perspectives regarding the importance of cybersecurity insurance, mapping the level of use of cyber insurance and in terms of coverage policy in their organizations.

Some tips and approaches are also provided to help in conducting self-assessments and raise awareness in terms of information and data protection, cyberattacks and threats, cyber insurance, and cloud security.

¹"ISACA Survey: Cybersecurity Attacks Are Rising During COVID-19, But Only Half of Organizations Say Their Security Teams Are Prepared for Them," ISACA

²"OnRisk. A Guide to Understanding, Aligning, and Optimizing Risk, 2020, 2021, 2022," The Institute of Internal Auditors

Highlights

We conducted a survey about cybersecurity threats with respondents from 23 industries. This survey was intended to provide insight in tackling cybersecurity as one of the key emerging risks. Moreover, through this survey, we also see the trend of migration to the cloud and concerns regarding these efforts from a cloud security point of view.

74%

believe that IT security policies and procedures has been implemented effectively

68%

believe that cyber attack will happen in the next 12 months

31%

attack in the form of malware

25%

attack in the form of phishing

36%

security protocols need to be updated

22%

privacy policies need to be updated

46%

operational disruption considered as the worst impact of cyber attack

29%

financial loss will be the worst impact of cyber attack

25%

respondents stated that their organization have cyber insurance, which covers risk of data destruction and business interruption

44%

use cloud services, for the following reasons:

38%

speed and ease of access

35%

cost efficiency

27%

data security

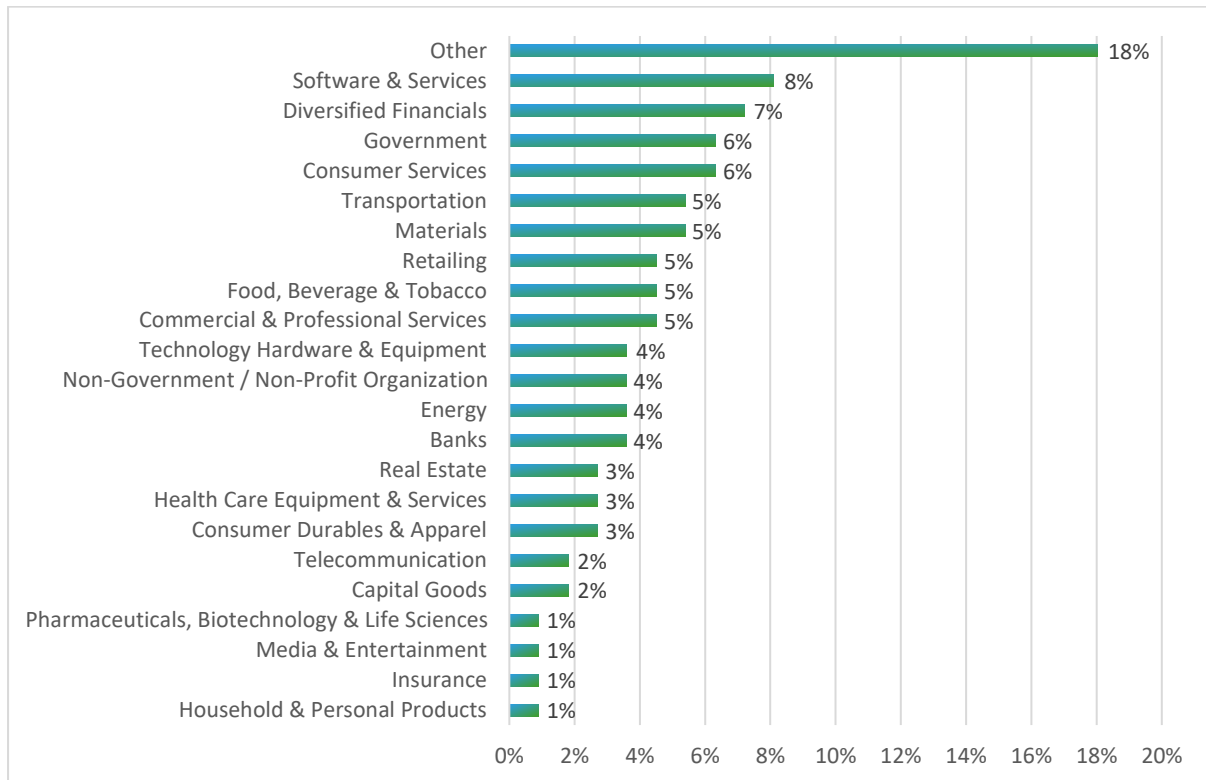


RESPONDENTS

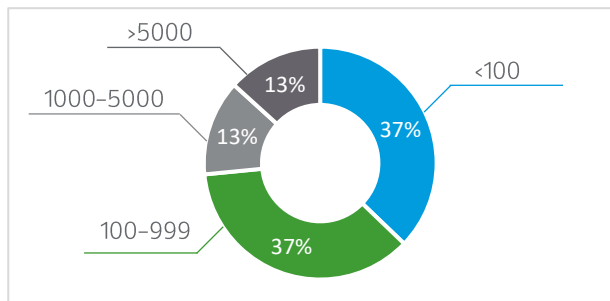
There were 113 respondents on this survey that came from various industries, 14% respondents are from consumer discretionary (retailing, consumer services, consumer durables & apparel), each 12% respondents are from Information technology (software & services, technology hardware & equipment), financials (Insurance, banks, diversified financials), and Industrials (capital goods, commercial & professional services, transportation) – all from Indonesia. The survey was fielded at the mid of 2021.

Respondent Demographic

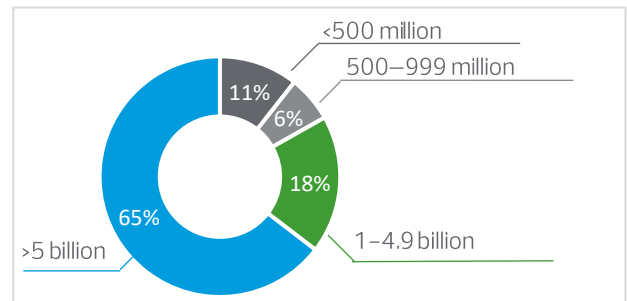
Industry



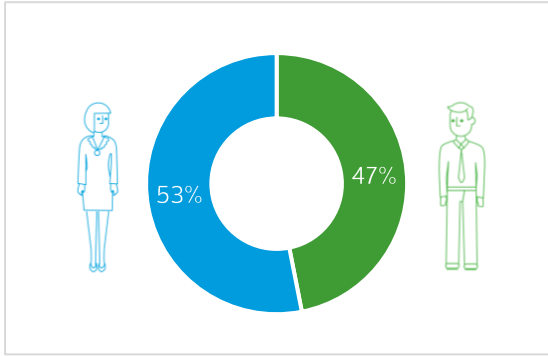
Size of Organization



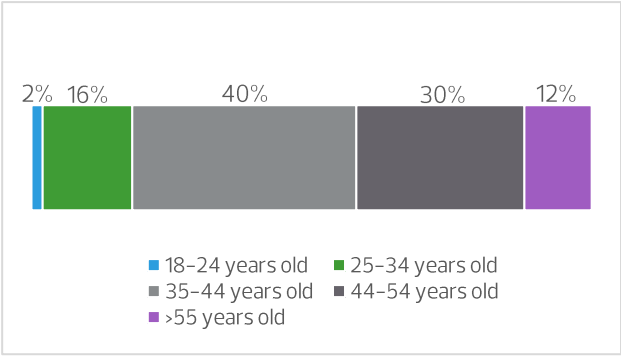
NUMBER OF PEOPLE



ANNUAL REVENUE (in Rupiah)



GENDER



AGE

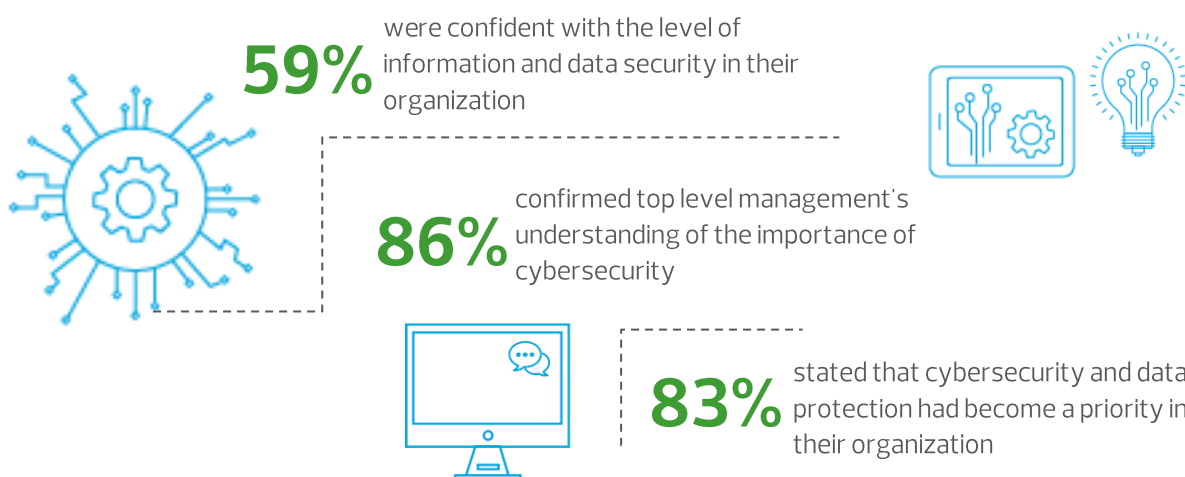
INFORMATION SECURITY AND DATA PROTECTION

The COVID-19 pandemic is changing the threat landscape in the mid-market due to the rapid large-scale shift to remote work environments and a greater reliance on the internet to stay productive. Many organizations have no experience managing such transitions, and security vulnerabilities are almost inevitable. Criminals are quick to strike, unleashing a number of attacks ranging from widespread malware and viruses to targeted phishing attacks.

Cybersecurity awareness for virtual interaction trends

With data breaches at record highs in 2019³, organizations were vulnerable even before the global pandemic hit, but effective communication about behaviours is critical now more than ever. These aren't your normal remote work concerns because this is not a normal situation. It's not just your employees staying at home, but also their spouses, roommates, parents, and children. They're also working at a time when people are most vulnerable to malicious actors seeking to take advantage of misinformation and uncertainty. This puts sensitive organization data, and the privacy of employees themselves, at risk.

Related to the increase in virtual activity at work, we asked respondents about the level of confidence in the security of information and data in their organizations.



While cybersecurity and data protection has been on boards' agendas, organizations face broad challenges to the effectiveness of cybersecurity, which must be addressed on priority. This reflected by the survey result showed that 86% of respondents confirmed top level management's understanding of the importance of cybersecurity and 83% of respondents stated that cybersecurity and data protection had become a priority in their organization.

Information security and data protection governance

Management leaders should understand and reinforce the importance of formalizing and cultivating the owner accountability principle for data security risk. This principle states that the resource owners (e.g., business process, application and data owners) are accountable for protecting the organization's information resources, its business processes and outcomes.

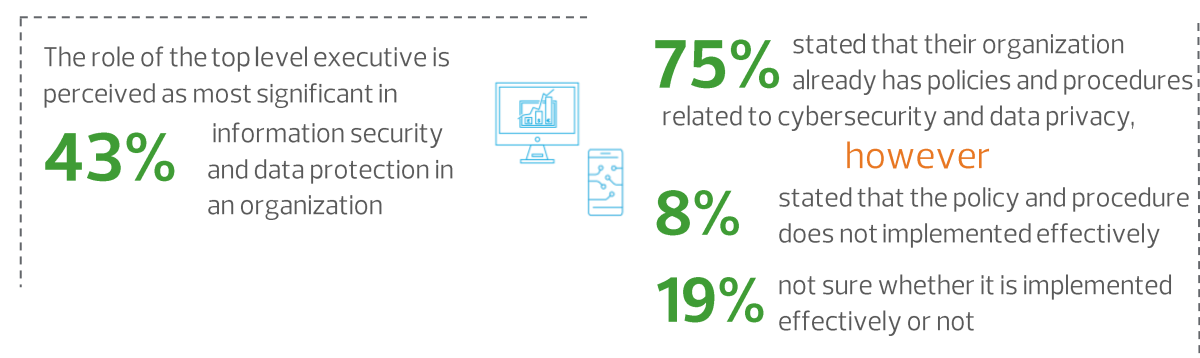
The role of the top level executive is significant according to the survey which 43% perceived that they are the most important party in charge of data security in their organization, and followed by the IT Division, which was 28%.

³ <https://www.riskbasedsecurity.com/2020/02/10/number-of-records-exposed-in-2019-hits-15-1-billion/>

As one of the main components of cybersecurity and data privacy, policies and procedures play a very important role as part of organizational governance. 75% of respondents stated that their organization already has policies and procedures related to cybersecurity and data privacy, however some of them were not sure about the implementation, some even stated the policies and procedure does not implemented effectively.

Policies don't mean much if they aren't communicated properly. Driven by the pandemic, an in-depth understanding of cybersecurity and data privacy is needed at this time by all employees, especially to increase staff awareness not to put sensitive organization data, and the privacy of employees themselves, at risk.

Employees are the weakest link and often the last line of defense. To protect this information, leaders must help their organizations communicate policies through regular training and refreshment. An informed workforce is key.



Insights from RSM Indonesia

Both the volume and value of customer and organizational information are increasing while costly data breaches are becoming more frequent. With the increasingly stringent data privacy laws, such as the General Data Protection Regulation (GDPR) applicable in the European Union and the Information and Electronic Transaction Law (UU ITE) applicable in Indonesia and will be strengthened by the Personal Data Protection Law (RUU PDP) which will apply in the future, organizations assume greater accountability about how this data is stored, used, and transferred.

However, it is not only external threats that put organizations at risk as most cyber breaches and data leaks are the result of human behaviour. Providing assurance of information security is critical to optimizing the value of an organization's information and preventing the costly consequences of breaches.

CYBERATTACKS AND THREATS

Looking back at 2020, it was a difficult year for many organizations for myriad reasons. The COVID-19 pandemic threatened employee safety and overall sustainability and required significant shifts in established business processes in many cases to maintain productivity. Unfortunately, these new processes added layers of complexity when just trying to keep the business moving, creating a perfect storm for hackers to exploit existing and new vulnerabilities.

From the beginning of the pandemic, cybercriminals launched a web of attacks with varying levels of sophistication intended to prey on users' sense of uncertainty. Hackers only intensified their attacks on middle market businesses when a large segment of organizations transitioned to a work-from-home structure, away from more secure internal networks and increasing reliance on the internet. Making that significant and sudden shift was necessary, but it left organizations more susceptible to attacks.

Experienced a cyberattacks

Our survey shows that cybersecurity threats are not just headlines, but occur, with even more significant potential in the future. This is seen from 12% of respondents who admit that their organization has experienced a data leak. This has the potential to be even greater because there are 22% who say they are not aware of it.

In addition, 16% of respondents admitted that they experienced a cyberattacks or demand during the last 12 months, even 7% of them experienced more than one incident.


This has the potential to increase significantly, as reflected in the results of a survey that asked about the potential risk of their organization being exposed to cyberattacks in the next year, where the survey stated that 68% of respondents felt that this might happen.

12% admitted that their organization has experienced a data leak

16% admitted that they experienced a cyberattacks or demand during the last 12 months

22% admitted that they are **NOT** aware of it

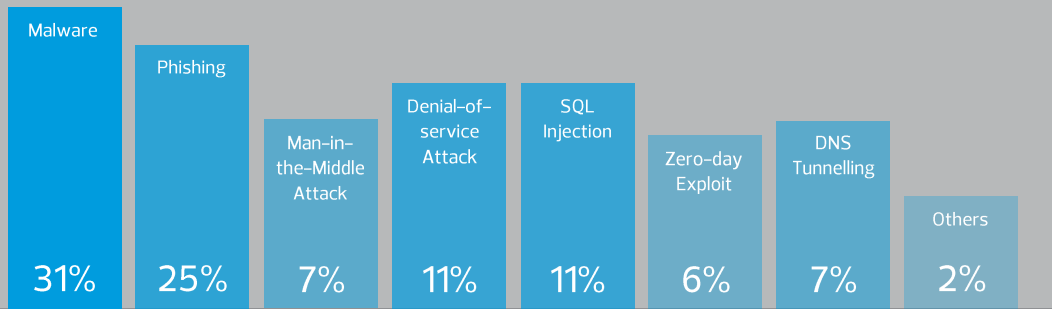
7% experienced more than one incident



68% felt that their organization might experience cyberattacks **in the next 12 months**

The COVID-19 pandemic is also changing the threat landscape in the mid-market due to the rapid large-scale shift to remote work environments and greater reliance on the internet to stay productive. Many organizations have no experience managing such transitions, and security vulnerabilities are almost inevitable. Criminals are quick to strike, unleashing several attacks ranging from widespread malware and viruses to targeted phishing attacks.

Cyberattacks that have potential to attack respondents' organization:

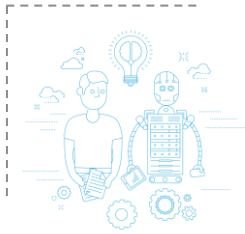


Impact of cyberattacks

Incidents of cyberattacks and large-scale intrusions illustrate the growing impact of cyberthreats activity on enterprise risk across all industry segments.

These risks are increasingly difficult to control and mitigate in IT and Organizational Operations environments. In an era of unprecedented uncertainty due to the pandemic, with so many devices spread across corporate networks, security professionals are challenging to keep up with security demands.

Our survey shows that the impact that is most felt by respondents is the occurrence of disruption in the operational activities of the organization and financial loss. Interestingly, most of respondents (70%) thought that the external party will be the most possible to carrying out the cyberattacks.



46% admitted that the impact that is most felt is **the occurrence of disruption in the operational activities of the organization**

29% admitted that they feel the impact of **financial loss**

70% thought that **the external party** will be the most possible to carrying out the cyberattacks



Reporting and follow-up on cyberattacks

Our survey results show that almost of respondent report cyberattacks incidents to their IT Division and 39% reported it to top level management. Only 5% of the respondent stated that they reported the incident to the Security/IT Security team.

The organization took various actions in response to the security breaches report. Almost half of respondent stated that the organization take reactive action as respond to security breach conducting a review of their IT system security, while others took steps by increasing their IT security.



49% thought that the external party will be the most possible to carrying out the cyberattacks

5% stated that they reported the incident to the Security/IT Security team

45% of the organization take reactive action as respond to security breach conducting a review of their IT system security

24% of the organization took steps by increasing their IT security

10% of the organization take steps to use third party services



Actions organization has taken to address cybersecurity threats

Many middle market organizations are active in their efforts to address cybersecurity threats. Based on the results of our survey, most notably have updated their organization's internal process, consisting of 36% of respondents reporting proactively updating the security protocols and 22% of them updating privacy policies.

Things that need to be done to improve cybersecurity in your organization:

36% Update the security protocol



9% Agree to all choices



22% Update our privacy policy



4% Add data security staff



13% Engage data security consultants



3% Others



13% Purchase new or upgrade software



Middle market organizations had a lot to contend since 2020—unprecedented changes were necessary to business processes as organization adapted to a pandemic environment, and cybercriminals were quick to strike with a record-high level of success. However, it's clear that middle market organizations have been making strategic changes to keep up with new risks, and that focus will need to continue and sharpen moving forward to address threats that are certain to continue evolving over time.



Insights from RSM Indonesia

With the number of entry points into organizations increasing and doubling, recent high-profile breach headlines, and exacerbated by the pandemic, it is not surprising that the topic of cybersecurity is becoming a major focus area today. Most organizations divide cybersecurity risks into two main categories: external and internal. External covers risks such as hacking and data breaches, while internal focuses on IT control environments, patching, and data leaks.

CYBER INSURANCE

With the number of breach attempts and successful breaches surging, cyber insurance has never been more valuable to middle market organizations in Indonesia. A well-defined and properly scoped policy can help organizations better protect critical data and systems and provide the necessary support to quickly recover from a potential breach.

Cyber insurance has steadily grown to become a key pillar of an effective cybersecurity approach. Even in recent years, many organizations may not have necessarily been completely familiar with how policies work or what coverages were available. However, we are now seeing some signals that the middle market is better embracing cyber insurance as a key protective measure.

Our survey found that 25% of respondents currently use a cyber insurance policy to protect against internet-based risks, with the majority focusing on policies related to preventing the risk of data destruction, hacking and business disruption. Meanwhile 57% do not have it and 17% of them are not sure about the existence of cybersecurity insurance in their organization.

The benefit of cyber insurance

Cybersecurity insurance is designed to offset recovery costs that an organization would have to pay in the event of a security incident. It can also offset a variety of non-IT business costs associated with a cyberattacks such as reputational damage (using PR firms/breach coaches) and legal fees. These are some of the qualitative benefits of cybersecurity insurance.

Another qualitative benefit often provided by cybersecurity insurance is accessibility to experts employed by or contracted to the underwriter and/or broker. Not only are these incident response or forensic services, but many cybersecurity insurers also have direct access to security experts for legal, PR and law enforcement contacts. Additionally, some insurers provide expertise and resources in planning, response, and recovery strategies. These resources can augment your existing team or in cases where they don't exist in-house, improve your ability to respond and recover.

Organization carries a cyber insurance policy

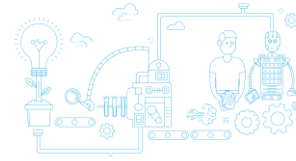
A cyber insurance policy is meant to be a supplement to traditional liability insurance, which typically does not offer coverage for cybersecurity incidents. Organizations must know where any coverage gaps exist and how the two policies interact to ensure that the desired level of protection is met.



"Cybersecurity insurance is entirely a reactive product. It will not prevent a cybersecurity breach or immediately reduce the impact on the delivery of services to your end users. Therefore, you must continue to invest in your security program alongside your cybersecurity insurance considerations."

Cybersecurity insurance is risk transference. It represents a purely reactive incident response activity and does not negate the need for investment in prevention and recovery, but it can be an important part of a comprehensive cybersecurity program. Technology leaders must understand cyber insurance's intended role, the costs associated with it and the limitations inherent in the coverage. Management leaders must be included and aware of discussions with cybersecurity insurance providers.

57% DID NOT HAVE any cybersecurity insurance in their organization



25% currently use a cyber insurance policy to protect against internet-based risks, with the majority focusing on policies related to preventing the risk of data destruction, hacking and business disruption

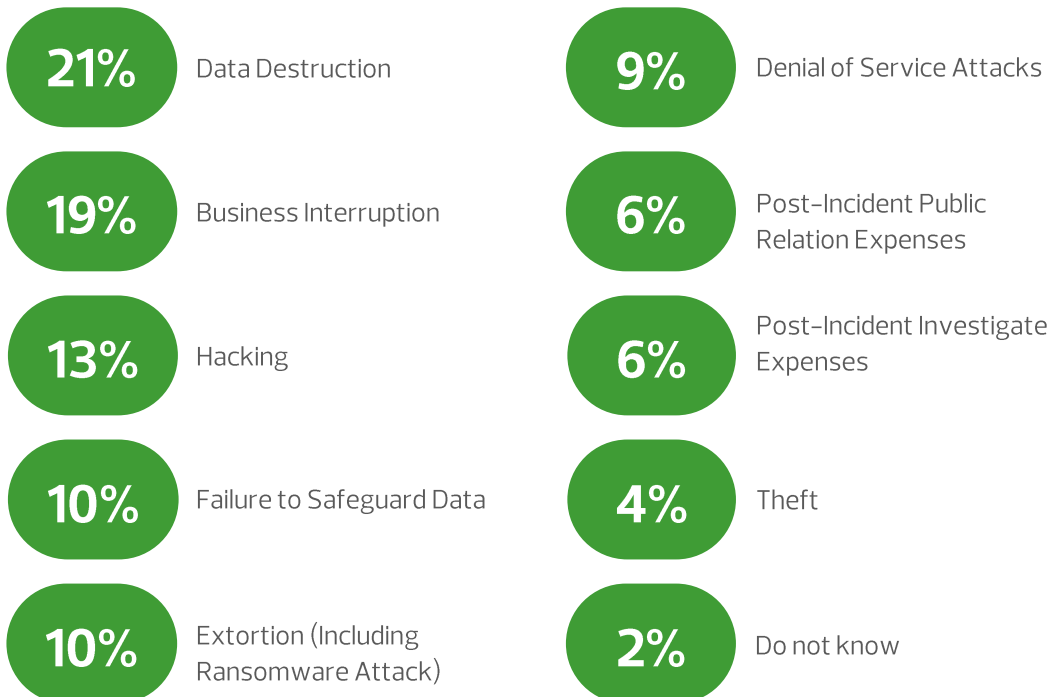
18% were not sure about the existence of cybersecurity insurance in their organization


Risks and exposures of cyber insurance

Cybersecurity insurance policies protect organizations from losses due to security incidents. The nuance to these agreements can be complex and filled with exceptions. To receive the expected benefits from cybersecurity insurance, executive leaders must be part of the process.

Cyber insurance policies are designed to be very broad and modular, with several potential options available to meet the specific needs of an organization. In our survey, respondents reported that their cyber insurance policies covered the most frequently coverage for data destruction (21%) and business interruption (19%). Followed by coverage against hacking (13%), cyber extortion (10%) and failure to safeguard data (10%).

The risks or exposures the cyber insurance policy that the respondents company covers:





In the current threat environment, cyber insurance is an imperative protective measure for middle market organizations. The financial, reputational, and regulatory impact that breaches often create can be extremely harmful, and a well-designed cyber insurance policy can help lessen those damages. However, as with any insurance product, organizations must be careful when establishing or renewing a cyber insurance policy to ensure that critical systems and data are protected as intended.

Insights from RSM Indonesia

Cybersecurity insurance is a transfer of risk but can play an important part of a comprehensive cybersecurity program. Tech leaders must understand the intended role of cyber insurance, the costs associated with it, and the limitations inherent in coverage. Management leaders should be involved and aware of discussions with cybersecurity insurance providers.

Prior to purchasing a cyber insurance policy, consider asking a series of questions to understand the exact limitations of coverage. We recommend some common questions that can help when you want to start discussions with your insurer:

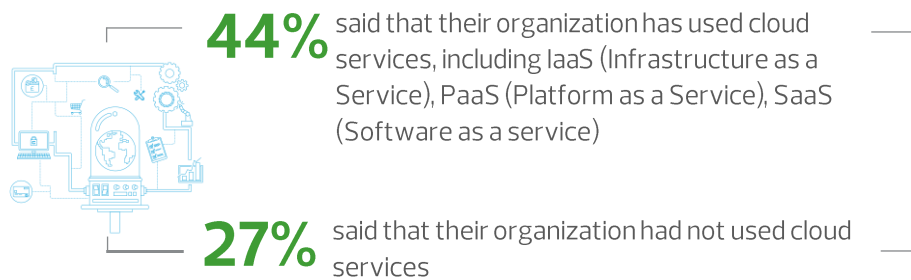
1. If we get exploited as the result of a security failure of an integrated third party, are we covered?
2. If we get exploited as the result of an unpatched system, are we covered?
3. If we get exploited as the result of a zero-day vulnerability in one of our software applications, are we covered?
4. Are there any geographical limitations or restrictions on the coverage?
5. Are there any technological limitations or restrictions on the coverage?
6. What is the minimally acceptable level of security you expect the organization to have and what is deemed acceptable proof of those controls?

The goal in this line of questioning is to completely understand where there may be gaps in the coverage. You can then decide to either accept that level of risk or put in other controls to minimize or prevent it from being exploited.

MIGRATION TO THE CLOUD TO ENSURE DATA SECURITY

The cloud has been an extremely valuable tool for middle market organizations; and at this point, almost every organization leverages the cloud in some manner. Many organizations use the cloud to gain control over data or increase access and visibility into information, but it is also gaining traction as a security tool.

With the increasing scale of many cloud providers, they can deliver security capabilities that may be out of reach for middle market organizations coupled with storage options that can typically meet a variety of business needs.



The reasons why organizations move or migrate data to the cloud

Cloud computing plays a strategic role in enabling digital business, as it addresses common IT constraints, such as slower time to value, limited resources and maintenance, and incompatible systems.

Cloud computing (particularly in the form of SaaS) frees IT from running systems of record for the business and enables IT staff to focus their time and energy on systems that support innovation and growth. Freeing up IT staff time to focus on these systems can increase the return on investment that comes from IT initiatives, potentially increasing profits, and competitive advantage.

Based on the results of our survey, it was found that 38% of respondents said they migrated to the cloud because of the need for speed and ease of access, very slightly different from 35% who stated the goal for cost efficiency. While 27% need the cloud due to their organization's focus on data security.

38% said they migrated to the cloud because of the need for speed and ease of access

35% said the goal for cost efficiency

27% showed their organization needs the cloud due to their organization's focus on data security



While the cloud may not be for everyone, it should at least be evaluated as a potential protective measure for sensitive data. In almost all cases, the cloud provides better access, organization, and security for data, but cost can become an issue. However, some of those cost pressures may be alleviated through a due diligence process that evaluates multiple providers to best match expectations with capabilities.



Insights from RSM Indonesia

Organizations are looking to cloud computing for scalability, efficiency, and cost reductions. Despite its many benefits, the cloud also opens significant vulnerabilities for organizations, such as data loss, data breaches and outages, or service disruptions.

As more processes and sensitive data are moved to the cloud platform, cloud risk assurance is a top priority for the Organization. Further, with greater business-led IT, various parts of the business are purchasing cloud services without going through the IT organization and thus, potentially bypassing the necessary approval processes.

This increases confusion about who is responsible for data protection, especially in organizations struggling with the visibility of third-party cloud providers. With only a few providers holding a large share of the cloud market, the effects of unintentional vendor lockouts can pose challenges to third-party vendor management, contract management (including audit rights clauses), and transparency about how and where an organization's data resides being saved.

To mitigate cloud security risks, we recommend that organizations implement stronger SLAs and contracts, using strong data encryption, and regularly auditing cloud provider facilities. In addition, clearly defining the provider's security responsibilities early in the process and regular monitoring is critical to risk mitigation.

CONCLUSION AND RECOMMENDATION

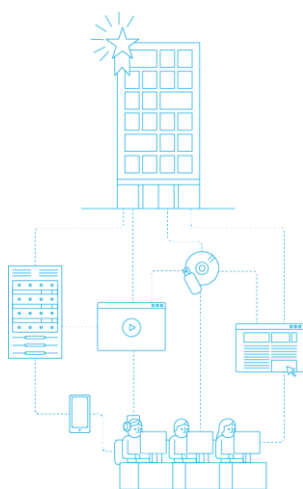
As the IT risk universe continues to grow – particularly in the areas of cyber security, information security and data protection – the role of IT audit and IT risk management in identifying key risks and mitigating controls is critical to success of the organization and its ability to digitalize. From reshaping engagements to expanding into new areas of coverage, IT audit and IT risk management must proactively keep pace with technological transformation in the organization.

With the emergence of new technologies and evolving IT project delivery procedures, and learning from the uncertainty caused by the pandemic, we anticipate IT audits to continue to adapt. To be well positioned to keep pace with future demands, IT audit must not only remain agile in identifying IT risks but also in its ability to modify approaches to provide the assurance required.

In dealing with IT risks including cyber and information security, we recommend several key insights that can help executives to light the bulb, especially to increase cybersecurity awareness in their respective organizations.

INFORMATION SECURITY AND DATA PROTECTION

- Establish procedures and controls to deal with potential data breaches
- Map key controls and measure the effectiveness of controls to mitigate data loss
- Prioritize patching as a critical IT security initiative, and keep it up to date
- Define the implications of the ITE Law and the RUU PDP
- Understand more about PII, what information has been collected and how to use it properly
- Pay attention to where data is stored and who has access to it
- Consider the involvement of third parties in the business, and ensure their level of compliance with applicable data privacy regulations



CYBERATTACKS AND THREATS

- Start paying attention to the frequency of patching
- Use an antivirus that suits your organization's needs and make sure it's always up to date
- Train employees and raise employee awareness to deal with phishing attempts, hacking and data leakage
- Focus on collaboration between the audit function and other assurance functions (security, compliance, legal, and head of data) in dealing with cyber risk
- Mapping the potential impact of cybercrime on your organization
- Think about doing penetration testing



MIGRATION TO THE CLOUD TO ENSURE DATA SECURITY

- List what data your organization currently stores in the cloud
- Think about what sensitive information your organization has outsourced to the cloud platform
- Set how to manage access to sensitive data in the cloud
- Define who can access data and platforms
- Determine who is responsible for the data
- Define the right criteria for selecting cloud product offerings

RSM INDONESIA

Plaza ASIA Level 10,
Jl. Jend. Sudirman Kav. 59
Jakarta 12190 Indonesia
P. +62 215140 1340
F. +62 215140 1350
[E. contact@rsm.id](mailto:contact@rsm.id)
www.rsm.id

RSM is represented in Indonesia by the following member firms: Amir Abadi Jusuf, Aryanto, Mawar & Rekan; PT RSM Indonesia Konsultan; PT RSM Indonesia Mitradaya; PT RSM Indonesia Mitradana. RSM's Indonesian member firms work closely together within Indonesia. Each firm is a separate and independent legal entity and a member of the RSM network and trades as RSM.

Each member of the RSM network is an independent accounting and consulting firm each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London, EC4N 6JJ.

The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.
© RSM International Association, 2021

THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING

