LATAM CISO
Report 2023

CYBERSECURITY

insights from Industry Leaders

LATAM CISO

Duke UNIVERSITY

For more information, please contact **info@latamciso.com**

LATAM CISO Duke University

Credits

Center for Cybersecurity Policy and Law

- Ari Schwartz
- Belisario Contreras
- Alex Botting

Duke University

- David Hoffman
- Daniel Rodríguez Maffioli
- Andy Kotz
- Sofia Bliss-Carrascosa
- Spencer Reeves

Digi Americas Alliance Members

aws CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google LUMU

netskope paloalto NETWORKS tenable Trellix TREND MICRO

Table of Contents

Foreword

David Hoffman, Steed Family Professor, Duke University
Andy Kotz, Researcher, Duke University
Belisario Contreras, Coordinator, Digi Americas Alliance

The LATAM CISO 2023 Cybersecurity Report provides insights from industry leaders regarding the level of cyber resilience among various organizations in the Latin American region. LATAM CISO is a multistakeholder and interdisciplinary network of cybersecurity professionals that aims to gather and coordinate input from members to shape the priorities of cybersecurity in the Americas and strengthen their overall security posture. This report was created to identify gaps in security, as well as the needs and limitations of organizations in Latin America that are preventing them from achieving a better stance against cyberattacks.

The Latin American region suffers more than 1,600 cyberattacks a second, which is why it is imperative that organizations toughen their capabilities to protect themselves from this growing environment of cyberattacks and security risks. The report is intended to provide decision makers from both the public and private sectors with insights to help them understand their vulnerabilities and focus their efforts and resources on the areas within their country that need the most support.

To this end, a survey was conducted among chief information security officers (CISOs) and other manager-level positions in 195 organizations from different sectors of all sizes. Among those surveyed, 21% work at a small organization (1–100 employees), 24% work at a medium organization (100–999 employees), and 56% work at a large organization (over 1,000 employees). The most heavily represented industries were financial services (24%), government (23%), and professional services (10%).

Over 70% of respondents reported that the number of cyberattacks on their organization has increased from the previous year, demonstrating that despite increased cybersecurity efforts, the attacks are persisting. The report begins with an assessment of organizations' budgets, types of attacks, number of attacks, risk assessment frequency, multi-factor authentication (MFA) deployment, security awareness trainings, and other factors that affect the cybersecurity capabilities of organizations. The report concludes with a set of recommendations that will contribute to improving cybersecurity and resilience in the Latin American region. The recommendations focus on each data collection category and suggest actions based on the findings. For example, the data collected demonstrate inadequate investment in regular security risk assessment. An increase in governmental campaigns to create cybersecurity frameworks requiring organizations to conduct risk assessments more frequently can enable the identification of vulnerabilities.

This report will enable organizations to thoroughly examine their cybersecurity capabilities and understand the next steps needed to increase their resilience against attacks. Overall, the report found that while efforts are being made to fortify cyber capabilities, threats continue to persist. Consequently, organizations must continue to pay more attention to their vulnerabilities and how they can address them.

How Latin America and the Caribbean Can Combat Cyberattacks in the Financial Sector

Eric Parrado, Chief Economist, Inter-American Development Bank
Diego Herrera, Lead Specialist for Financial Markets, Inter-American Development Bank

The region receives more than 1,600 cyberattacks per second. Response teams, cooperation mechanisms, formal education, and greater investment are some of the actions that governments can take to support the private sector in mitigating risks.

Latin America and the Caribbean are one of the regions with the highest incidences of cyberattacks in the world. According to data from various cybersecurity firms, the region receives more than 1,600 cyberattacks per second. To get an idea of the proportion, during the first six months of 2022, global ransomware distribution attacks reached 384,000, with the region accounting for 14% of the total .[1] The correlation between the size of the economies and their level of digitization with the number of cyberattacks is undeniable: Brazil receives more than half of the cyberattacks, followed by Mexico (23%), Colombia (8%), and Peru (6%).

Cybersecurity becomes relevant if one takes into account that the economic damage from cyberattacks could exceed 1% of the gross domestic product (GDP) in some Latin American and Caribbean countries. If attacks on critical infrastructures are observed, this figure could reach up to 6% of GDP.[2] Furthermore, according to data from the Inter-American Development Bank, 7 of 32 countries analyzed in a study had a protection plan for their critical infrastructure, and 20 had a Computer Emergency Response Teams (known as CERT or CSIRT).[3]

The financial sector is a critical infrastructure in the region. Recent advances in the digitization of the sector position it as one of the most relevant in terms of cybersecurity. The figures show that after the start of the pandemic caused by COVID-19, the number of financial operations using digital media increased substantially in the region. For example, in Colombia, according to data from the Colombian Financial Superintendence, 72% of financial transactions are carried out through digital channels, such as mobile phones or the internet, by 2021.[4] Furthermore, according to data from Banco de la República (the Colombian Central Bank), 50% of the businesses included in a survey adopted electronic payment channels.[5] An emblematic case is Brazil, where, through the payment system of the Central Bank of Brazil—PIX—more than 2,800 million monthly transactions are carried out, of which 75% correspond to payments between people (P2P), with the participation of almost 800 institutions providing financial services. To give an idea of the magnitude, PIX has 133 million users in Brazil. Data from a survey carried out by the cybersecurity company PSafe showed that 844,821 attempted attacks on the PIX infrastructure between January and June 2022, showing the importance

1. Información disponible en: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics. Consultado el 24 de enero de 2023.
2. Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA). 2020. "Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe". Disponible en: http://dx.doi.org/10.18235/0002513. Consultado el 24 de enero de 2023.
3. Ibidem.
4. Superintendencia Financiera de Colombia y Banca de las Oportunidades. 2022. Reporte de Inclusión Financiera (RIF) 2021. Disponible en: https://www.superfinanciera.gov.co/jsp/10111791. Consultado el 25 de enero de 2023.
5. Información disponible en: https://www.banrep.gov.co/es/blog/efectivo-pagos-electronicos-tiempos-pandemia. Consultado el 25 de enero de 2023.

of cybersecurity in infrastructure as relevant as payments. In other words, although digitization offers significant advances in financial inclusion, it also imposes challenges in terms of cybersecurity.

The great advantage of the financial sector is that it is one of the most organized sectors in terms of cybersecurity in the region. From a public perspective, financial authorities in countries such as Chile take operational risks in financial sector infrastructures as a component of financial stability analysis. The participation of various entities (finance ministries, central banks, bank superintendencies and commissions, securities, pensions, and insurance, among others) in collegiate groups, such as financial stability councils, gives flexibility to generate public policies and regulatory changes that mitigate cyber risks in the jurisdictions of the region. From a private perspective, it shows how the sector cooperates at the regional level to share information about cyberattack incidents at the individual level of entities in the sector. The role of regional unions, such as the Latin American Federation of Banks (FELABAN), is important in consolidating this type of effort and having databases on incidents.

Recommendations to combat cyberattacks in the financial sector

To combat cyberattacks, it is advisable to take public policy actions that guide the private sector in achieving risk mitigation. Three basic recommendations are made below.

Initially, it is recommended that a national cybersecurity incident response team (CSIRT) be established to improve the levels of preparation and response to cyberattacks. At the national level, it is useful to generate databases on computer incidents for key infrastructures, such as those of the financial sector, and to generate policies that encourage the dynamic exchange of incident information between entities and sectors. It is also essential that the national CSIRT belong to platforms such as CSIRT Americas, which allow the sharing of information and generating cooperation mechanisms at the regional level. The financial sector should be part of these initiatives. Similarly, it is necessary to train officials of financial and public entities in the sector. Education must be accompanied by constant updating of trends and technologies that allow mitigation of cyber risks. Finally, these two issues must be accompanied by investment in technology that allows for mitigating cybersecurity risks and their materialization. It is estimated that the financial sector in the region invests 10% of its technology budget in this relevant topic. As the sector becomes more digitized, more investment may be required.

In conclusion, the formalization of the CSIRT, national and international cooperation mechanisms, formal education, and investment in cybersecurity will allow our financial sectors to mitigate the risks associated with a more digital business with a vocation for consumer protection.

Cybersecurity and the Financial Sector in Latin America and the Caribbean

Giorgio Trettenero Castro, Secretary General, Latin American Federation of Banks (FELABAN)

The Latin American Federation of Banks (FELABAN) was born as the representative of Latin American banks to adhere to one of the highest cybersecurity standards in the region. FELABAN, with a focus on cybersecurity and bank fraud specifically, aims to improve the efficiency and stability of the Latin American financial system as well as cybersecurity capabilities in the region as a whole.

We see communication and collaboration, or rather the lack thereof, as one of the biggest threats to the cybersecurity landscape. As banks transform into a more digital environment, fraud and security breach mechanisms evolve in parallel. Although a bank, or a country, may understand these new threats, the rest of the region needs time to catch up, and often does so after it is too late.

FELABAN, with the aim of forming strong regional connections and fulfilling its mission as a banking union, has taken the initiative to develop an innovative Latin American collaborative project that aims to build bridges between banks throughout the region and to form an open line of communication. Sharing best practices and key information in banking security, banks from 11 different countries have been able to mitigate the risks inherent in day-to-day financial operations. This pilot project, which began in October 2022 and ended in January 2023, builds on a new collaborative model and paves the way for information exchange among banks in the region.

The preliminary results of this pilot have been exceptionally positive: a new dynamic for information sharing has shown the banks involved the responsiveness we can achieve by working together, and there is still plenty of room for growth. Institutions are sharing relevant information that is changing the way they view banking security. A case of fraud or an attack is no longer an isolated event. Due to this higher level of exchange, we have found patterns in different cases of fraud, even between countries. Certain fraud techniques are based on various channels of interaction between countries. By increasing communication and working on understanding fraud in another's country, one can improve the response to fraud in one's own country.

As we look to the future, we hope to incorporate stronger technology assets into our regional projects. Under the current dynamics of this collaboration model, we believe that sharing certain technologies will be easy and effective. By implementing a collaboration model that leverages current technology and artificial intelligence, we can empower a bank or country to defend quickly against a cyber breach. This solution will enhance cybersecurity capabilities and provide a more efficient and effective response to potential threats.

As we continue to analyze the data from this initial pilot project, focusing on LATAM, we are extremely optimistic about its potential. As a region, Latin America faces many similar, if not exactly the same, threats. By forming a collectively responsible group, the financial sector, or any industry, will strengthen its collective cybersecurity capabilities as well as its ability to respond to attacks and grow in the future.

The CISO as Storyteller? Getting the Attention of the Board

Seán Doyle, Lead, Centre for Cybersecurity, World Economic Forum

In February 2022, a cyberattack on commercial satellite services in Ukraine caused electricity-generating wind farms to fail across Central Europe. Just over six months earlier, in July 2021, supermarkets in Sweden were forced to close their doors after a cyberattack on an IT services provider based in Florida, USA, disrupted the operations of its international clients. In both cases, the rolling flow of disruption was neither predicted nor predictable. The first target of these attacks was shared services providers. They were not household names and did not appear to have a systemically important role in the digital ecosystem. However, the consequences spread across sectors and borders.

These incidents show how different technologies across a multitude of organizations now have the same common dependencies or weaknesses. This means that the impact of cybersecurity incidents can cascade from organization to organization and across borders. The risks this creates are systemic, contagious, and often beyond the understanding or control of any single entity. Systemic risks can be difficult to predict and quantify, and even more difficult to manage. The threat environment has become more volatile, and attacks have greater disruptive potential. Organizations need to split their attention between defense from cyberattacks and resilience after a cyberattack occurs.

Try putting yourself in the shoes of the security teams at the electricity firm and the supermarket chain that were 'collateral damage' of the attacks discussed above. What could they have done to prevent this disruption? In all likelihood, the answer is "not much." Many technological dependencies are now difficult to see until they break. We can't prevent what we are unable to see. This means that more attention needs to be paid to resilience, the ability to recover from attacks or reduce the damage they can do.

World Economic Forum research, due for full publication in its Annual Cyber Outlook Report in 2023, also found a positive trend. Boards are more aware of cyber risks than ever before. This is partly driven by high-profile attacks across all sectors. Geopolitical disturbances in Europe have also brought the topic of cybersecurity onto board members' coffee tables as the threat of cyber war makes headlines in newspapers around the world. Boards are also being drawn to the topic by a growing body of regulation and the development of accepted principles for board-level governance of cybersecurity risk. This helps focus attention on the benefits of integrating cyber resilience into business processes and governance structures. Whatever the reason, the increased interest in cyber risk at the board level is an opportunity for CISOs in 2023.

What can the CISO do?

Boards are ready to listen to their cybersecurity teams. Successful CISOs can explain cyber risk in a way that makes sense to the board. They make the story of cybersecurity accessible to executives and translate cyber risk into metrics, such as profit and loss to operations or reputational damage, that business executives understand and can use to prioritize spending.

Starting your story with the geopolitical situation can be a good entry point for explaining why your organization might be targeted by criminals or how it can be impacted by disruptive attacks on other organizations. Showing business leaders how an abstract cyber risk would concretely look in their business allows boards to grasp the meaning of a cyberattack but also spread responsibility for cyber resilience beyond the information security team to business units.

Regarding resources, board-level support makes it easier to embed cyber-risk governance through the organization. If the board is interested in cyber resilience, then the rest of the business will follow. This can make the organization an asset to the CISO's team and not just a target to be defended. Our research indicates that boards are likely to feel more confident in the security of their organizations when cyber risk management is integrated into decision making and processes across their organizations. For example, some of the companies surveyed for the 2023 Global Cyber Outlook report include the CISO or members of their team on key bodies, such as audit, risk, and finance committees. In these cases, the CISO and their team become trusted advisors to the business teams and support the secure development of new business processes.

Businesses are changing the way they use technology. This creates unseen technological dependencies and new cyber risks. The CISO's role will not become less technically complicated in 2023. However, opportunities to engage business leaders on the topic of cyber risk management are increasing.

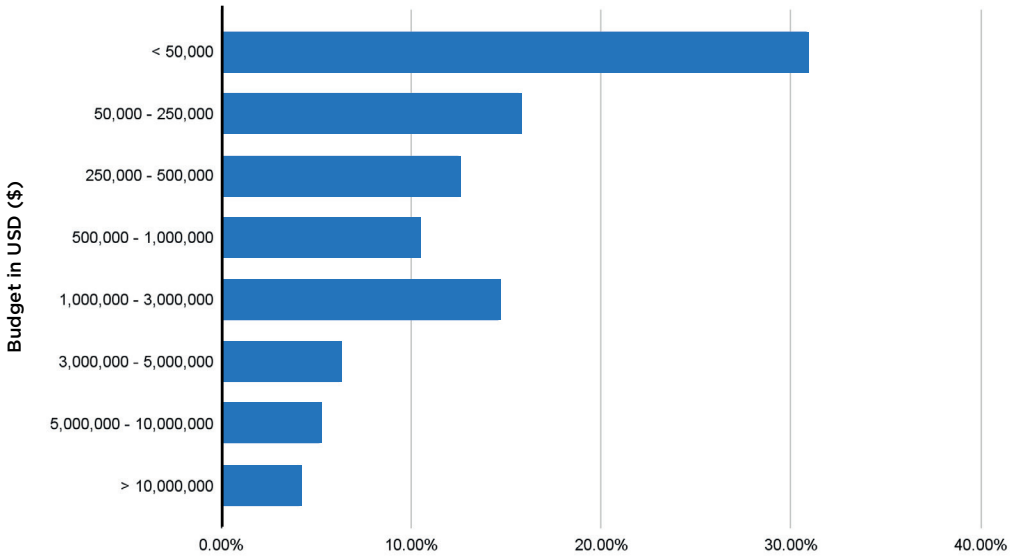

.fcb-popup {
position: absolute;
top: 0;
left: 0;
width: 100%;
height: 100%;
z-index: 10;
}

Findings

Dedicated Budget for **Cybersecurity**

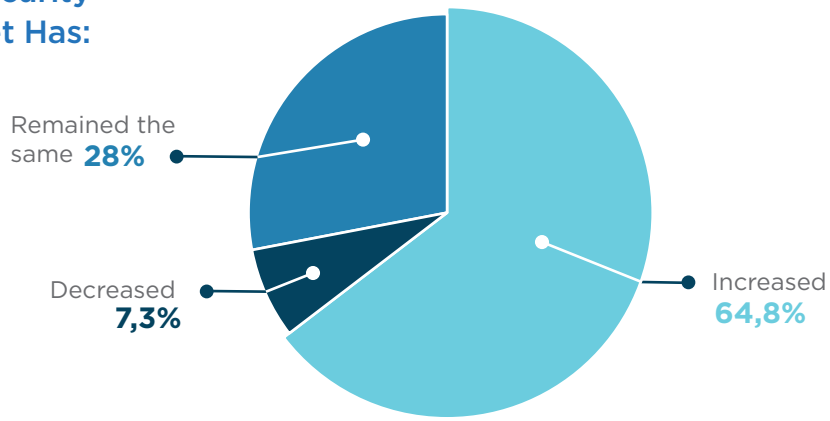
With regards to the budget for cybersecurity within the organization, 31% of the respondents report having a budget under $50,000 (USD), with a majority (59%) of organizations having a budget below $500,000. The cybersecurity budget had increased for 65% of respondents from the previous year, and the budget had decreased for only 7%. This shows a growing understanding of the importance of cybersecurity among these companies.

Q5. Cybersecurity Budget



Notably, the majority of organizations with a cybersecurity budget of less than $50,000 did not see an increase in their cybersecurity budget but rather remained the same, and in some cases (8.47%), their cybersecurity budget decreased. Considering that the group of respondents with budgets of less than $50,000 is the largest in the survey, and that most of those companies saw an increase in cyberattacks in the last year, it would be worthwhile to identify the reasons for the stagnation in the budget in order to effectively address those causes in the future.

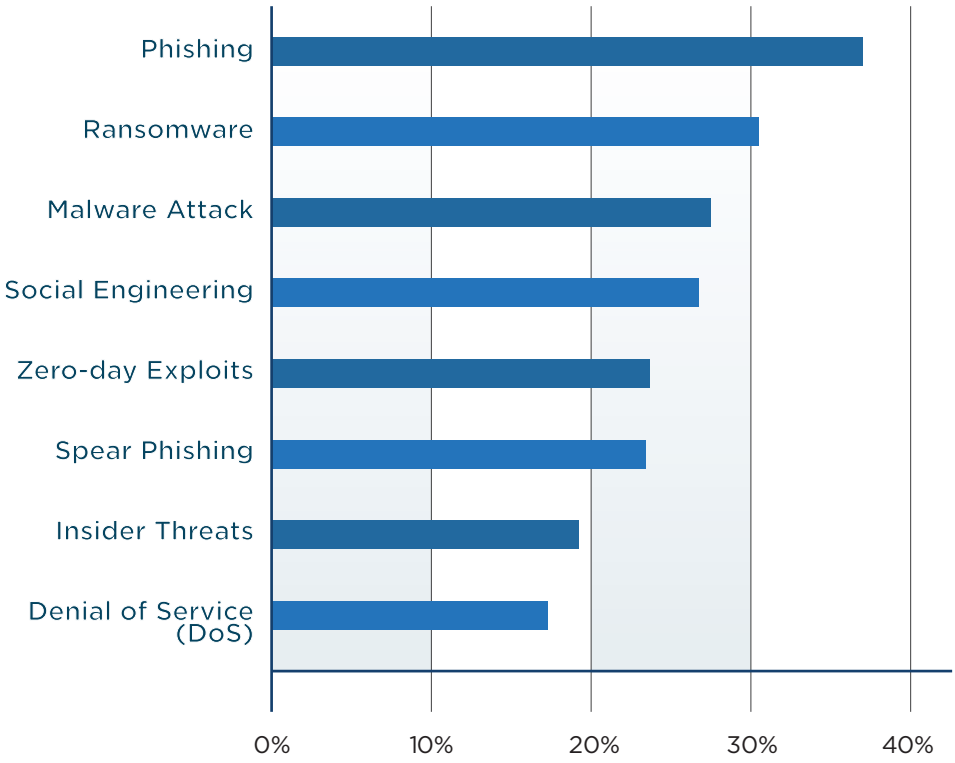
Q6. Cybersecurity Budget Has:



Types of Cyberattacks Faced

- Among the countless forms of cyberattacks, phishing, ransomware, and malware attacks are some of the most common. By understanding the most common types of attacks, cybersecurity teams can more efficiently combat them. Categories of attacks often overlap (phishing and social engineering), but comparing rankings of responses helps to understand what is of most concern to CISOs. When asked to rank the top five types of attack based on which occurs most frequently, 37% of respondents ranked phishing as number 1, with 98% of respondents choosing it as the top 5. The next most common responses ranked as number 1 were ransomware and malware attacks, with 31% and 28%, respectively. Further, 95% of respondents placed these two as the top 5.
- Interestingly, social engineering, one of the only "non-technical" forms of attacks, was ranked number 1 by 27% of respondents and in the top 5 by 95%. This highlights the importance of not only technical cybersecurity defenses but also ensuring good cyber hygiene among employees.
- Other notable forms of attacks mentioned as number 1 are zero-day exploits (24%), spear phishing (24%), denial of service (DoS) (17%), and IoT-based attacks (17%), among others.

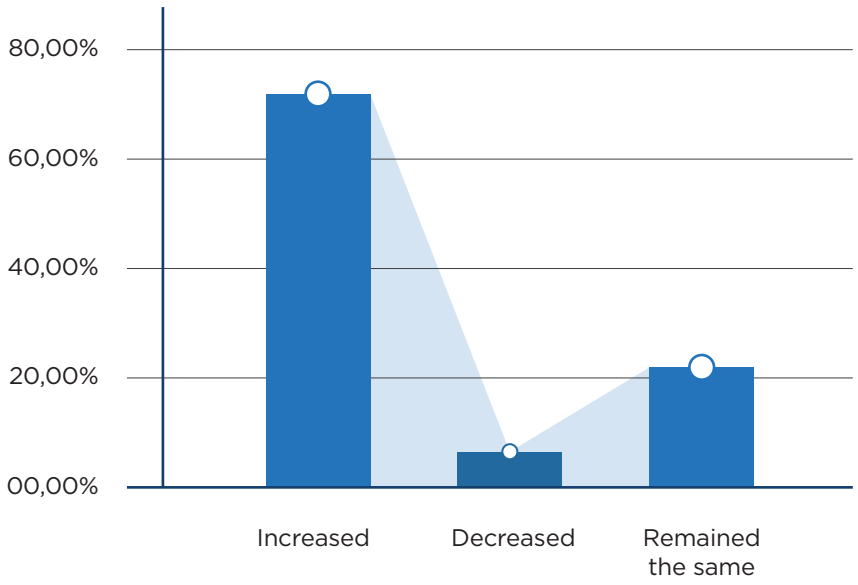
Q7. Most Common Types of Cyber Attacks



Cyberattacks Year over Year

- Ver 71% of respondents reported that the number of attacks on their organization had increased since the previous year. Only 8% of respondents reported a decrease in the number of attacks. With this much increase in such a short amount of time, the importance of security risk assessments, employee training, and other cybersecurity-related efforts has grown exponentially.
- More than half of the respondents of all industries considered have seen an increase in attacks, except for agriculture & mining, and the media & entertainment sectors. For the computers and electronics, consumer goods, manufacturing, travel & hospitality, and retail industries, every single one of the respondents reported an increase in attacks compared to last year, signaling a need for these specific sectors to enhance their cybersecurity defenses.
- More large organizations than medium or small ones (78% compared to 61% and 63%, respectively) perceived an increase in the number of attacks, reflecting how big organizations are usually a preferred target for cyber criminals. A reason for this might be the greater visibility but also the greater reputational consequences of an attack against big companies, which serves as leverage for criminals to achieve their goals. Another possible reason for this difference is that smaller organizations with low budgets might not prioritize monitoring the number of attacks.

Q8. Change in Attacks Since Previous Year

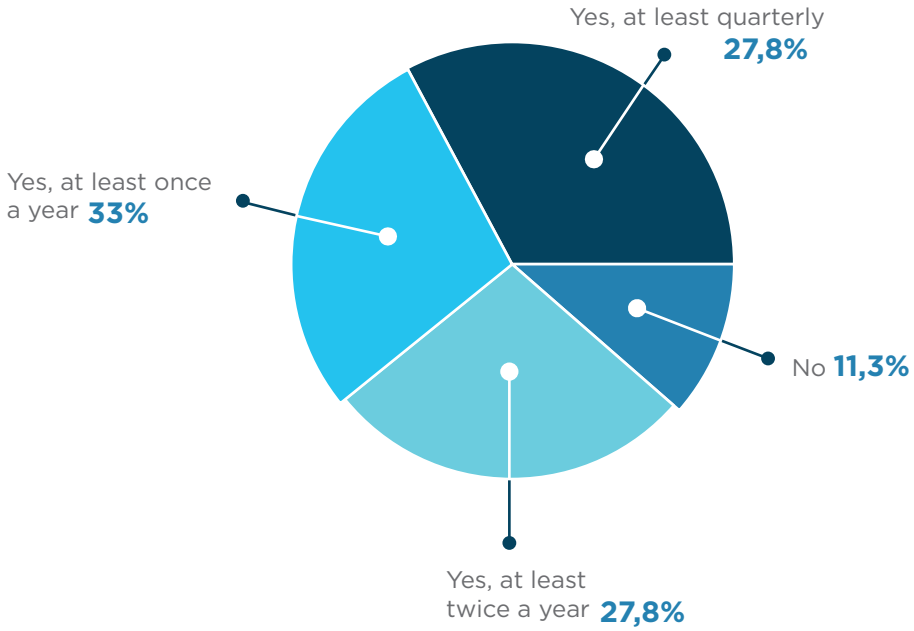


FINDINGS

Security Risk Assessment Frequency

- Many organizations are taking the increasing threat of zero-day attacks seriously, and room for growth remains. Over half of all organizations (60.83%) perform security risk assessments only ‘at least once a year (33%)’ or ‘at least twice a year (28%)’. Only 28% of organizations perform these assessments at least quarterly. Given the frequency and hidden nature of zero-day attacks, regular security assessments are critical for identifying new zero-day vulnerabilities and preventing exploitation.
- Although the approach to zero-day attacks varies slightly among industries, the two sectors in particular stand out. Notably, 66.67% of the respondents pertaining to non-profit organizations reported not having carried out security risk assessments in the last 12 months, even when non-profits are equally exposed to cyberattacks as private companies or public entities.
- However, 40% of those surveyed in the healthcare sector did not carry out security assessments. The healthcare sector is particularly prone to cyberattacks due to the sensitivity and value of the patient data it collects.

Q9. Security Risk Assessment Frequency

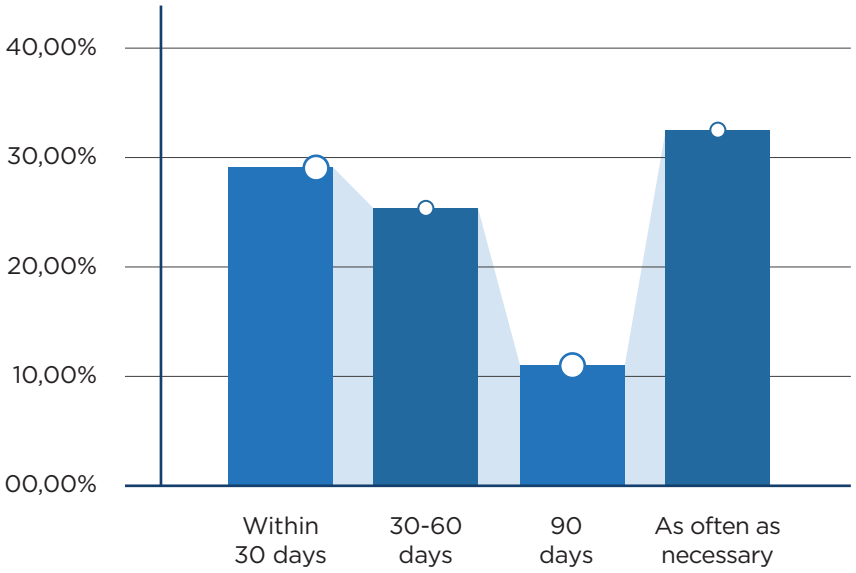


Frequency of Security Patches

- Most patches were applied within 30 days (29%) or 60 days (26%). Another 34% also stated that they applied patches 'as often as necessary'. In addition to organizational security patches, 65% reported patching third-party applications. Companies tended to rely on third-party software and application vendors to manage their operations. These applications often require periodic security updates, so they will not be used as vectors to access the companies' systems.

- Interestingly, the organizations with the lowest cybersecurity budget (0–$50,000) were less likely to patch third-party applications, with only 48.28% of them doing so. This makes it necessary to assess whether there is a correlation between the low budgets of organizations and their capacity to carry out these patches. One possible explanation is that smaller organizations do not have the technical and human resources to recognize when patches are needed, and/or have the resources to install them.

Q10. Frequency of Security Patches

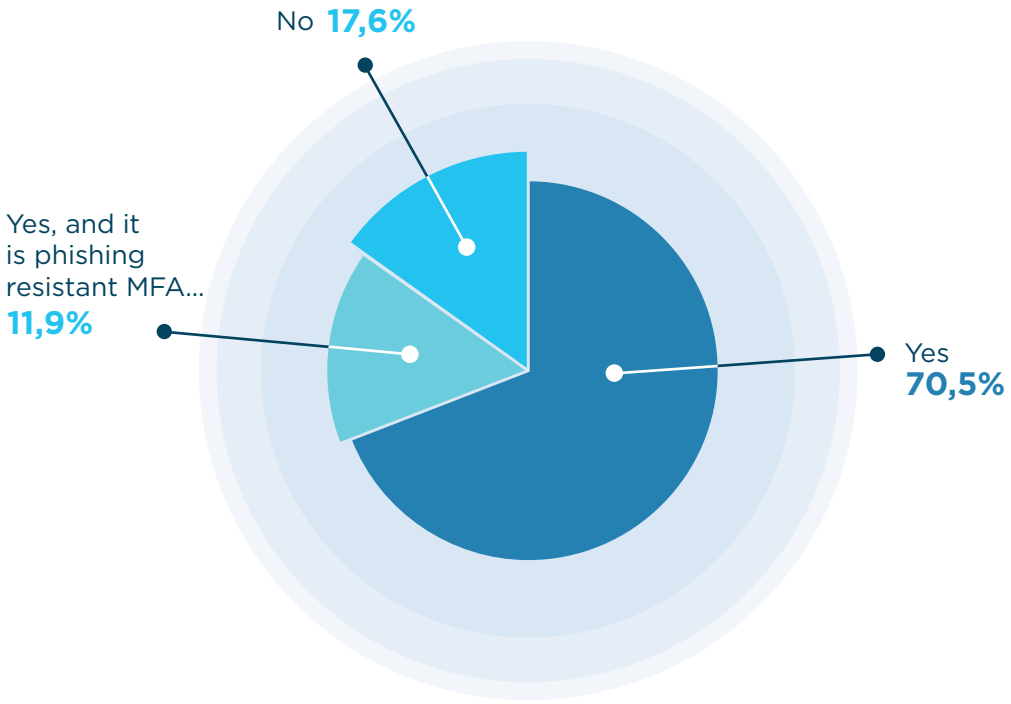


FINDINGS

Deployment of Multi-Factor Authentication

- One of the easiest ways to prevent, or at least mitigate, potential cyberattacks is to better protect employees' login and access information. Using MFA is one of the best tactics for this, as it helps ensure that an authorized user is accessing information, rather than some outside actor. Of note, 70% of respondents' organizations deploy some MFA, with an additional 12% deploying phishing-resistant MFA (such as FIDO or PKI).
- Surprisingly, large organizations were the most likely to not deploy MFA, with 19% reporting so. This is about 2 points above average, with only 13% of small organizations reporting that they do not deploy MFA.
- Organizations with budgets between $250,000 and $500,000 (96%) were the most likely to deploy some form of MFA.

Q12. Current Deployment of MFA

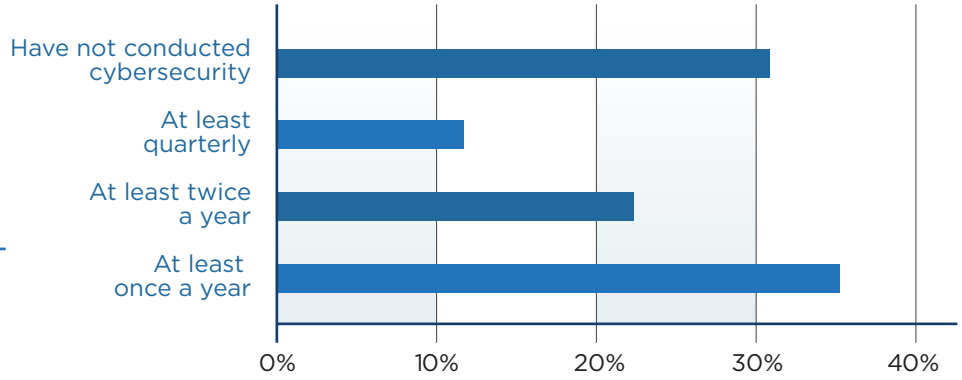


FINDINGS

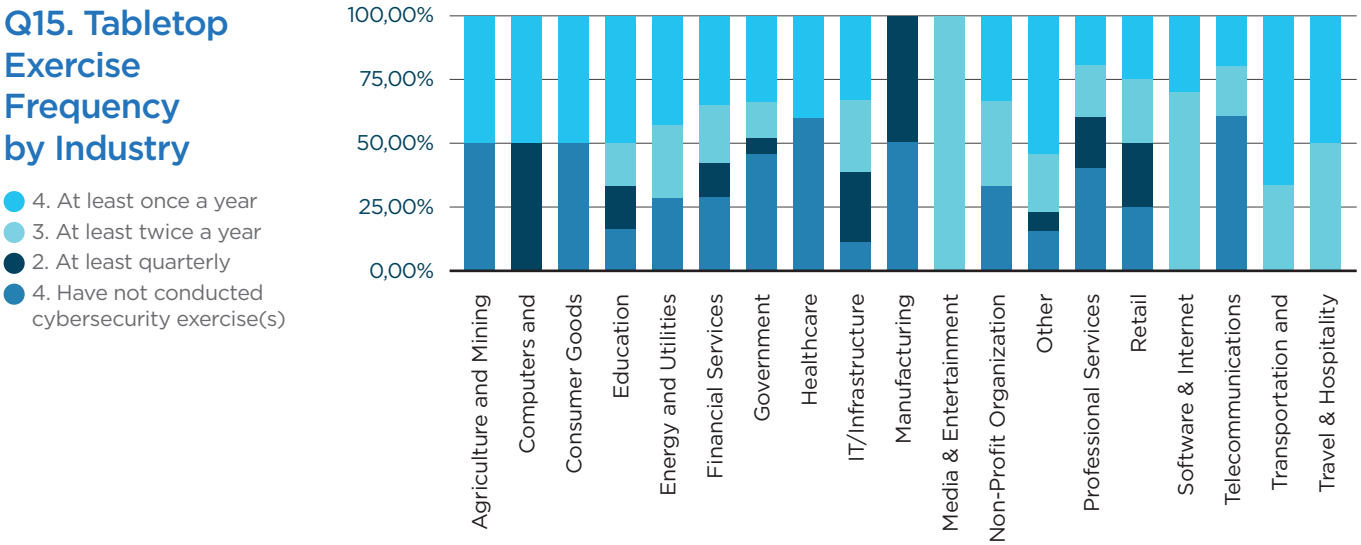
Tabletop Exercise Frequency

- Other forms of preparation are equally as important, such as cybersecurity tabletop exercises and security awareness training for employees. 30% of all respondents report that their organization does not conduct cybersecurity tabletop exercises. Another 35% report conducting such exercises 'at least once a year'. In order to be better prepared for incident response, organizations should be preparing these exercises more frequently.
- Certain industries report having not conducted cybersecurity tabletop exercises more than others. While on average 30% of organizations report having not done such exercises, certain industries report much higher rates, such as: Healthcare (60%), Professional Services (40%), Telecommunications (60%), and Government (46%). All these sectors affirmed perceiving an increase in the number of attacks in the last year.
- Small organizations (39%) and organizations with budgets below $500,000 per year, also report having not conducted tabletop exercises, most likely due to lack of resources.

Q15. Frequency of Tabletop Exercises



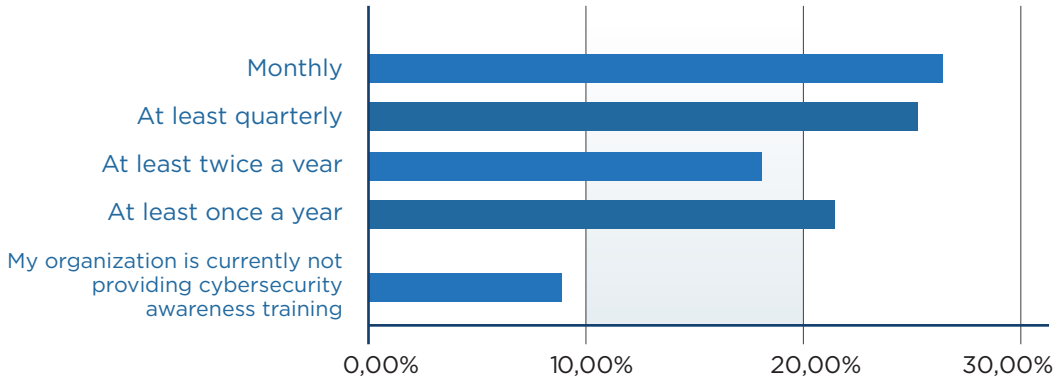
Q15. Tabletop Exercise Frequency by Industry



Security Awareness Training

- Over 50% of respondents reported providing security awareness training monthly (26%) or quarterly (25%), with others doing so at least twice a year (18%) or once a year (22%). Only 8% reported a complete lack of security awareness training.
- There was little variance between size or industry, except for small organizations, which did not provide training as often as medium- and large-sized companies.

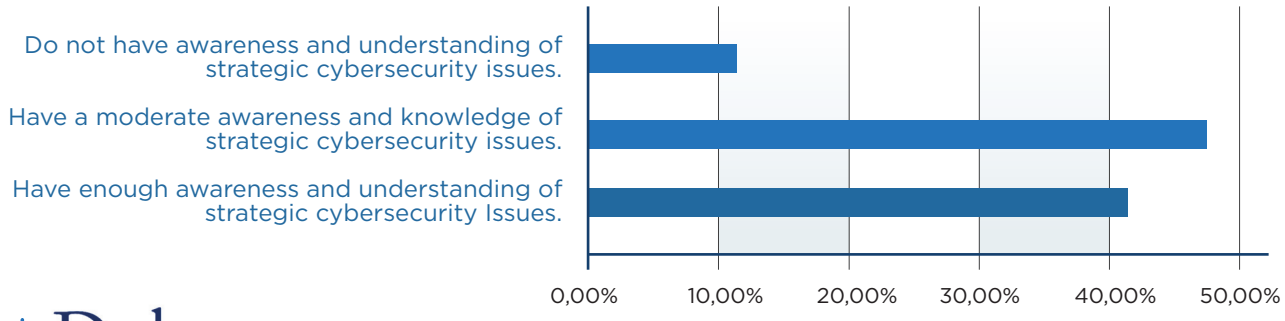
Q16. Frequency of Security Awareness Training



Trust in C-Level Executives

- When asked about C-level executives, 47% of respondents believed those executives had a 'moderate awareness and knowledge of strategic cybersecurity issues' and 41% believed they have 'enough awareness...' Further, 11% of respondents believed their C-Level Executives 'do not have awareness and understanding of strategic cybersecurity issues.' The leadership team's awareness and understanding of these issues is extremely important to map out an organization's approach to cybersecurity. C-level executives should strive to be well-versed in cybersecurity strategy, or ensure those around them are.
- Small organizations had slightly less trust in their executives, but the differences were minimal among size, budget, and industry.

Q13. Trust in Board of Directors and C-Level Executives

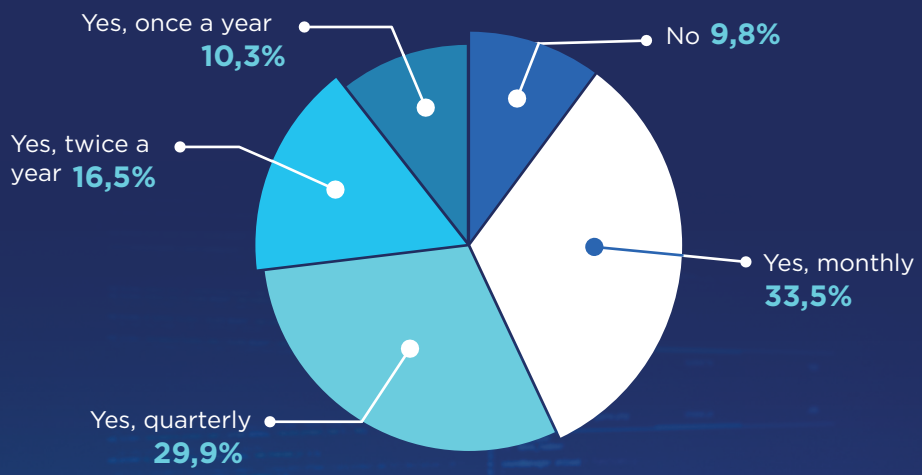


FINDINGS

Cybersecurity Report Frequency

- Many organizations provided reports to the board of directors and C-level executives about the state of cybersecurity. Over half of the respondents' organizations provided monthly reports (34%) or quarterly reports (30%), with an additional 17% issuing reports twice a year and 10% issuing reports once a year. Only 10% of the organizations provided no cybersecurity reports.

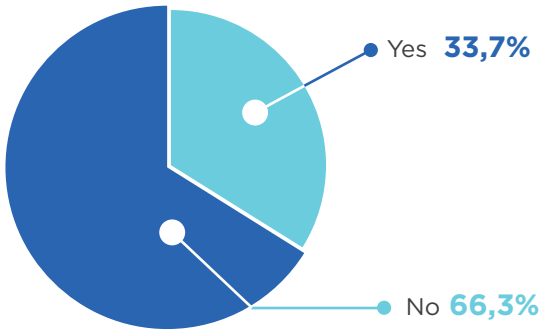
Q14. Frequency of Reports to Directors and C-Suite



Cybersecurity Liability Insurance

- In terms of other forms of preparation and response to cyber incidents, over 66% of respondents reported that their organization did not have any form of cybersecurity liability insurance. Liability insurance is another measure of executives' willingness to invest in cybersecurity.
- Notably, 85% of small organizations did not have cybersecurity liability insurance. To improve their resiliency position, it is crucial that smaller organizations work just as hard to prevent and mitigate harms.
- Companies with the lowest budget were less likely to obtain liability insurance, signaling that a low budget might be one of the main obstacles to accessing it.

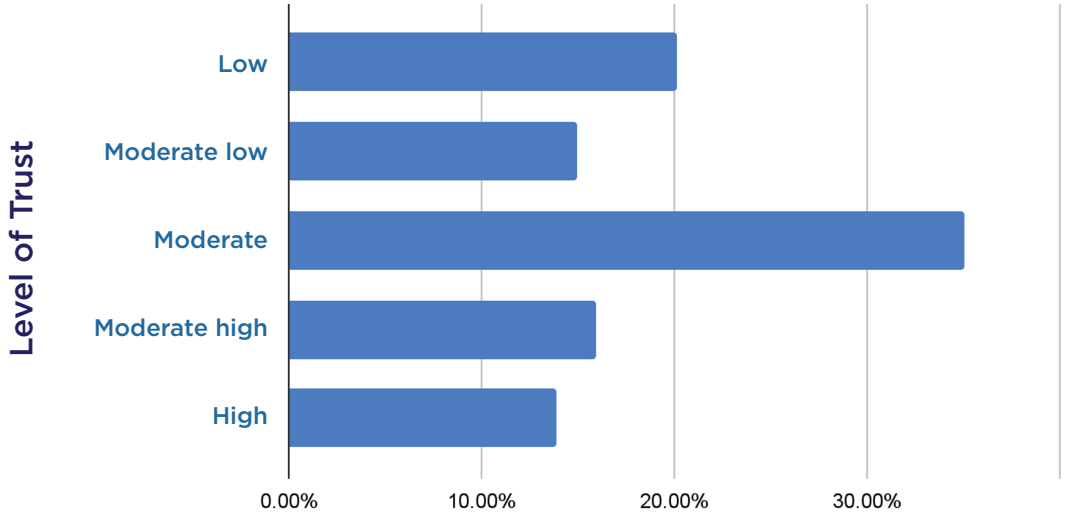
Q17. Cybersecurity Liabity Insurance



National Law Enforcement Agencies and National CERT

- Following a cyberattack or related cyber incident, organizations should contact national law enforcement agencies and/or the national CERT. Although most organizations know the proper procedures for this, 32% reported that they did not know whom to contact or how to contact them.
- Regarding national aid to cyberattack responses, 35% of organizations had low (20%) or moderately low (15%) trust in national law enforcement agencies and their national CERT. Another 35% reported moderate trust in the same agencies, with only 16% reporting moderate high trust and 14% reporting high trust.
- Non-profits (67%) and telecommunications (60%), as well as small organizations, reported the lowest levels of trust.
- The ability to work cooperatively with governments and government agencies in the wake of a cyberattack or related cyber incident is critical in preventing other similar crimes.

Q18. Trust in National Law Enforcement Agencies and CERT

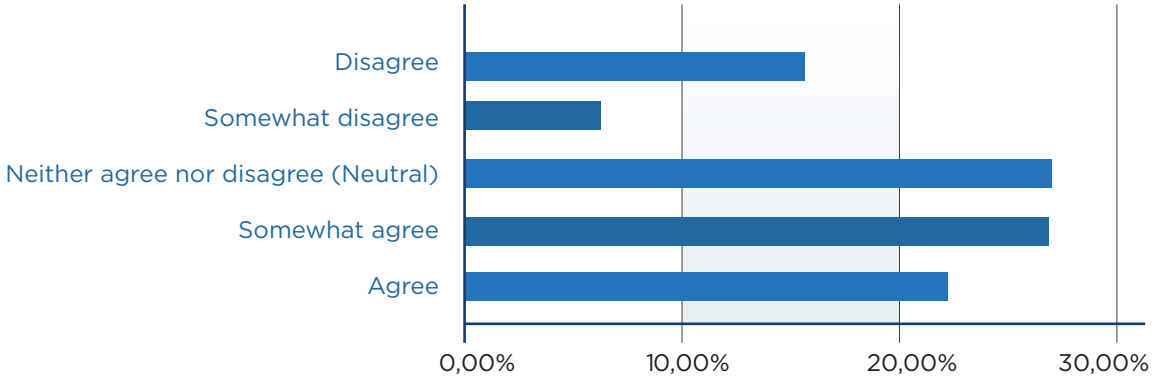


Inputs are Taken into Consideration for Public Policy, Regulation, etc.

- One possible explanation for the lack of trust in national law enforcement agencies and CERTs is that organizations do not feel as though their inputs are taken into consideration for the development of public policies, regulations, and other initiatives with a national impact. When asked if their organization's inputs were taken into consideration, 23% of respondents at least somewhat disagreed, with an additional 28% neither agreeing nor disagreeing. About 50% of the organizations at least somewhat agreed that their inputs were taken into consideration.

- Along with small organizations (26%), non-profits (67%), and telecommunications (40%) organizations also did not believe that their inputs were taken into consideration.

Q20. Inputs Are Taken Into Consideration



Public-Private Information Sharing

- Another possible explanation for a lack of trust or belief in cooperation is the lack of formal cooperation itself. About 51% of organizations did not belong to any public–private cybersecurity information sharing organizations, with little variation across industries or company size.
- Through continued cooperation and information sharing, both public–private and private–private, organizations can increase their cybersecurity capabilities and prevent large-scale cyber incidents from occurring. Cooperation must be inclusive and multisectoral.

Recommendations

RECOMMENDATIONS

Budget

Governments should work with organizations in their countries to identify the barriers to increasing cybersecurity budgets. Once the barriers are identified, governments can then develop tailored approaches to ensure that certain organizations that create risk to citizens and society have adequate assistance to properly protect data and networks. If small organizations do not have sufficient budgets to provide robust cybersecurity programs, governments should pursue government stipends and shared services targeted at those small organizations. Elements of these government efforts should include risk assessment, patching, and tabletop exercises.

Risk Assessment

The data demonstrate broad inadequate investment in regular security risk assessment. Governments should explore specific campaigns to create cybersecurity frameworks that require organizations to conduct security risk assessments continuously, including source code reviews in software development companies, enabling them to identify and address weaknesses in preparation to face the ever-evolving threat landscape. Since small organizations may have less visibility of risks, governments should pursue government stipends targeted to enable these organizations to conduct such assessments.

Types of Attacks

Phishing attacks may be a symptom of a larger category of business email compromise as well as the initial mode of delivery for the next two most responded attacks: ransomware and malware. Governments should explore training and shared services that can assist organizations in decreasing the risk of the compromise of business emails. Moreover, it is critical for organizations to learn and increase their resistance to realistic social engineering attacks. Therefore, governments should pursue policies that require organizations to regularly leverage red teaming. This security testing approach simulates attacks a threat actor may perform, including trying to influence employees to disclose information.

Patching

Governments should pursue policies that require software development organizations to inventory their products' components through a software bill of materials (SBOM), leverage software composition analysis (SCA) continuously to identify vulnerable components and take measures to communicate and mitigate the detected risks. Governments should also consider specific education campaigns across industries to implement cybersecurity frameworks that require applying patches as often as necessary. Moreover, governments should explore whether smaller organizations need access to shared services or government resources to effectively apply timely patches.

Break Silos

Government should encourage organizations to develop a strategy based on the use of solutions that eliminate cybersecurity silos, and instead rely on technology that coordinates/orchestrates existing defense solutions and allows them to extract additional value from these existing tools.

RECOMMENDATIONS

Compromise Assessment

Governments should encourage organizations in the private and public sector to systematically work to identify connections continuously with known malicious infrastructure and block them immediately to reduce business operation disruptions and other negative consequences.

Cybersecurity Operations

It should be recommended that organizations shift their approach to solving cybersecurity problems from a technology-only approach to one that blends cybersecurity operations plus technology, enhancing the visibility and orchestration capabilities of their current cybersecurity stack with mechanisms that offer operational feedback and build cyber resiliency.

Cloud Security

Many of the risks uncovered in the study can have cloud environments as their attack surface, where additional concerns like misconfigurations arise. Governments should pursue policies that consider these cybersecurity risks, but also enable organizations to leverage cloud native and augmented security controls to enhance their security strategies. The right balance between compliance and true risk management in the public cloud while benefiting from foundationally secure cloud infrastructure can be a good enabler for security strategies.

Multi-factor Authentication

Governments should pursue policies to encourage/require large organizations to implement MFA when accessing systems processing sensitive information.

Tabletop Exercise Frequency

Considering the constant threat of cyberattacks, governments should pursue policies that require organizations to effectively test their incident response plans. Such an assessment is possible with red teaming exercises. These refer to simulations of real-world scenarios in which a group of security analysts take on the responsibility of attacking the organization, while the response team in the organization assesses the security status and organizes, implements, and improves security controls.

Senior Management and the Board

The survey data reflect uneven confidence in the knowledge of C-suite executives. Governments should focus on providing clear expectations for the cybersecurity knowledge level of senior management and the board of directors.

Cybersecurity Insurance

Governments should investigate options to encourage organizations to obtain insurance that is effective at reducing cybersecurity risk. Governments should analyze whether there are insurance policies available that are affordable and useful to mitigate risk. Companies can leverage compromise assessment solutions to demonstrate cybersecurity maturity and reduce cyber risk policy costs.

Law Enforcement and CERTs

There is broad distrust across the region in working with national computer emergency response teams and law enforcement. National and regional CERTs should develop a collective strategy to address this lack of trust. One specific element of that strategy should be how governments should take into account private sector input into the policy development process.

Threat and Vulnerability Information Sharing

Governments should determine mechanisms to encourage all organizations to participate in information sharing bodies, such as sector-specific information sharing and analysis centers (ISACs).

LATAM CISO
Report **2023**

LATAM CISO

Duke UNIVERSITY