SRIT Outlook

Cyber Security Worldwide 2024

Contents

- Foreword
- 1. Threat Landscape
- 2. Global Trends
- 3. Country Vulnerability
- 4. Forecast for 2024
- 5. Emerging Challenges
- 6. Managing Cyber Future

Conclusion

Foreword

Leading business organizations today have recognized the importance of cyber resilience being key to operational sustainability and are being increasingly distinct from those grappling with cybersecurity challenges.

Geopolitical instability, rapidly advancing technologies and an increasing gap in organizational cyber capabilities reinforce the need to build resilience and prevent tactical business setbacks.

Cybersecurity Outlook for 2024 from SRIT is sourced from forward looking thoughts shared by leading security organizations, and dozens of experts across numerous security teams, who share our passion for cyber security.

These agencies and individuals are regularly on the frontlines of the latest and largest attacks, and know what organizations and security teams need to be thinking about in the coming year.

Therefore, we consider their opinions and assessments is the best leading indicator to the future.

This report is a consolidation of our learning and foresight in cyber security space around the world, and how the cyber future is unfolding in an ever dynamic threat landscape.

We hope our customers and partners shall find this beneficial to their business and clients.

Dr. Shubha Sunil
Executive Director & Cyber Security Practice Head
SRIT India

Threat Landscape

A stark divide between cyber-resilient organizations and those that are struggling has emerged. This clear divergence in cyber equity is exacerbated by the contours of the threat landscape, macroeconomic trends, industry regulation and early adoption of paradigm-shifting technology by some organizations.

Other clear barriers, including the rising cost of access to innovative cyber services, tools, skills and expertise, continue to influence the ability of the global ecosystem to build a more secure cyberspace in the face of myriad transitions.

These factors are also ever-present in the accelerated disappearance of a healthy "middle grouping" of organizations (i.e. those that maintain minimum standards of cyber resilience only). Despite this divide, many organizations indicate clear progress in certain aspects of their cyber capability.

This year's outlook also finds cause for optimism, especially when considering the relationship between cyber and business executives.

Compared to Last Year

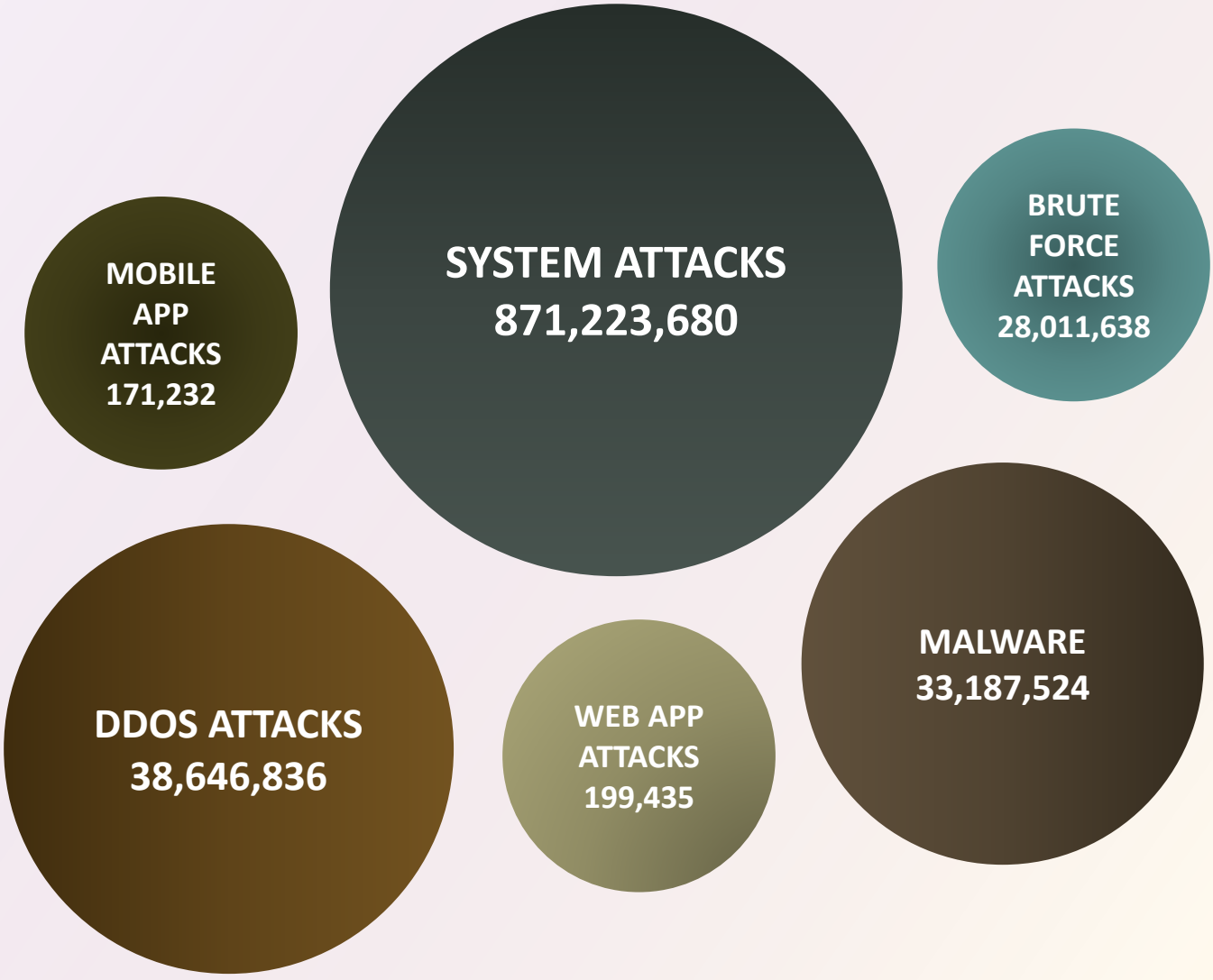
75%
Increase in cloud environment intrusions

110%
Increase in cloud-conscious cases

76%
Increase in victims named on eCrime leak sites

72%
Attacks motivated by ransomware

51%
Increase in cyber security budget allocation



Cyber Attack Vector Trends

During the quarter Jan-Mar 2024, system misconfiguration attacks were the most prevalent, which aligns with global trends in cyber threat activity where malware attacks, and more specifically ransomware, were most rampant.

Misconfiguration attacks can be attributed to limited investment in cybersecurity, outdated systems, default system login credentials, and limited cyber risk visibility, thereby raising the susceptibility of the critical information infrastructure sectors to cyber attacks.

Global Trends

Alignment between cyber and business is becoming more common

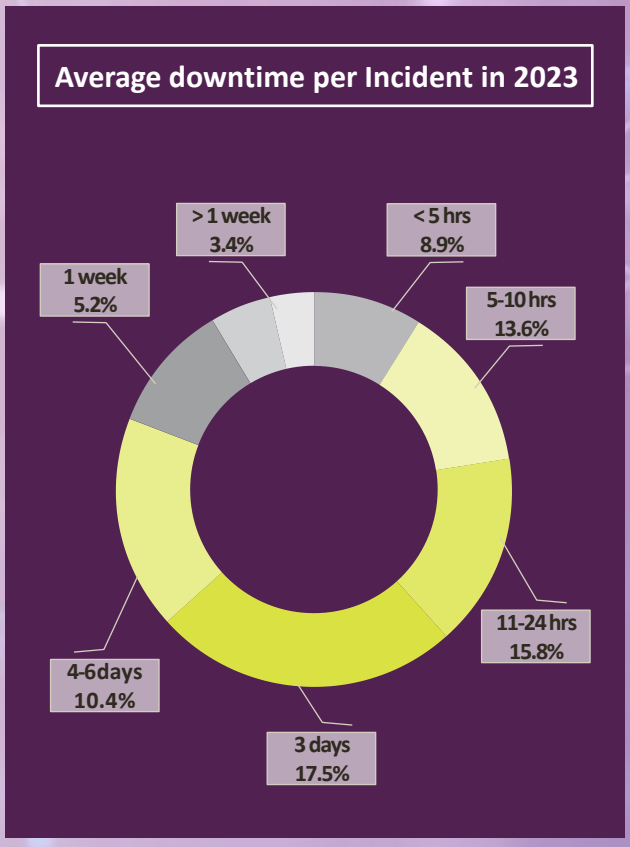
There is a clear link between cyber resilience and CEO engagement. Organizations who are leaders and innovators in cyber resilience trust their CEO to speak externally about their cyber risk Organizations (including both business and cyber leaders) must continue to invest in and maintain an awareness of essential security fundamentals. The smartest organizations realize that the highest barrier to cyber resilience is transforming legacy technology and processes that support core business operations.

Migration to modern programming languages by malware authors

Malware authors continue to develop in programming languages such as Go, Rust, and Swift due to the low level capabilities, large standard library, and easy integration with third-party packages. These languages and ecosystems enable rapid development of complex malware, making it cheaper to write new malware to evade detection. This means a churn in toolsets used by actors, and a corresponding need for new detection signatures. Unfortunately, these modern languages make reverse engineering tasks more difficult.

Developers targeted in supply chain attacks via software package managers

In recent years, supply chain attacks against the Node.js package manager such as IconBurst have demonstrated how threat actors target software developers. For example, a developer is compromised by installing a malicious package, which gives a threat actor access to the developer's source code, and allows the actor to add a backdoor. This is a low-cost, high-impact attack. This is likely to continue to grow, particularly as threat actors shift to other, less monitored package managers.



Revival of ancient techniques

Some attackers are using ancient techniques like that the case mentioned in 2013, in a blog post about using undocumented SystemFunctionXXX functions instead of cryptography functions in the documented Windows API. This technique didn't become popular until Q4 2022, when several security researchers began discussing it and releasing code snippets on GitHub. At that point, more malware samples implementing this technique started popping up. The technique was not covered in detection rules because the hypervisor is not often used in many countries.

Rise of disruptive hacktivism

Last few years showed a resurgence in the volume of hacktivist activity, particularly associated with threat actors expressing support for a side Russia or Ukraine during the ongoing conflict. Likewise, recent conflict between Hamas and Israel has been accompanied by a flurry of hacktivist activity. Observed activity includes distributed denial-of-service (DDoS) attacks, data leaks, and defacements. Notably, in both contexts hacktivist groups exhibit greater than average capabilities, and significant alignment with narratives and objectives of the state they claim to support

Extortion operations continue

Extortion operations remain likely the most impactful form of cyber crime to enterprises and societies worldwide. Despite a stagnation in growth during 2022, advertisements for stolen data and extortion revenue estimates indicate that this threat is growing in 2023, and we anticipate this growth will continue in 2024 without a significant, market-wide disruption.

Cyber insurance premiums remain steady

In the fluctuating insurance market, a strong correction in the cyber insurance market over the past few years, the market is starting to soften. With more entrants in the market and insurers with ambitious cyber growth goals, the competition is expected to provide much needed relief to the rising premiums the industry has been seeing. Insurers may broaden coverage in other ways to compete in this new landscape.

Major Attacks in Recent Past

2021 JBS Ransomware

On May 30th 2021, cyber criminals breached the JBS network with ransomware, disrupting plants in the USA, Canada and Australia. JBS had to pay UD 11Mn to the attackers.

2021 Robinhood Data Hack

On November 3rd 2021, data of 7 million users of this stock trading app was stolen and held to ransom by cyber criminals. The hackers accessed this data through social engineering.

2022 NHS Breach

On 4th August, Advanced, a key supplier of digital NHS services like patient check-ins and NHS 111, suffered a ransomware attack from an unknown hacking group.

2022 Nvidia Breach

On 23rd February, Nvidia, a major microchip producer suffered a data breach which saw source code fall into the hands of cyber criminals.

2022 Costa Rica Ransomware

The first attack was in mid-April, with 27 government bodies with digital tax service and the IT system for customs control were crippled. Second attack was on 31 May targeting SSF.

Country Vulnerability

In an ever increasingly connected world, cyber threats are a growing concern for every country.

Cybercriminals constantly launch sophisticated attacks, targeting organizations and governments anywhere. With the rise of connected devices and the Internet of Things (IoT), cyber-attack risks have expanded across all sectors.

It is crucial for countries to enhance their cybersecurity defences due to the severe consequences of cyber-attacks, such as financial losses, damage to reputation, service disruptions, and threats to national security.

Understanding a country's cybersecurity readiness is vital in today's environment. Using data analytics and machine learning, we can assess each nation's cybersecurity strengths, weaknesses, and areas needing improvement.

Exploring the cybersecurity rankings of different countries can help us make informed decisions, encourage global cooperation, and work towards a safer digital world for everyone.

The analysis is based on a comprehensive dataset encompassing various indices, including the National Cyber Security Index, Cybersecurity Exposure Index, Global Cybersecurity Index, Cyber Resilience Index, and the Final Cyber Safety Score.

We can gauge a country's preparedness and susceptibility to cyber threats by examining these metrics.

Key Findings

Finland, Norway, and Denmark lead with Final Cyber Safety Scores above 92, showcasing robust cybersecurity infrastructure and proactive measures.

The United Kingdom and Sweden maintain scores above 89, underscoring effective cybersecurity preparedness and resilience.

Japan and the United States demonstrate strong defences against cyber threats with Final Cyber Safety Scores above 88.

Australia and Austria exhibit commendable cybersecurity frameworks, with a final score above 89.

Honduras, Bolivia, and Venezuela face significant cybersecurity challenges, scoring below 42.

Algeria, Ecuador, and Kyrgyzstan confront growing cyber threats with scores below 52.

Sri Lanka, Panama, and Armenia exhibit vulnerabilities, with Final Cyber Safety Scores below 56.

Pakistan grapples with cybersecurity challenges, scoring 56.40, necessitating concerted efforts for enhancement.

Most Secure Countries

Rank	Country	National Cyber Security Index	Cybersecurity Exposure Index	Global Cybersecurity Index	Cyber Resilience Index	Final Cyber Safety Score
1	Finland	85.71	89	95.78	93.64	92.81
2	Norway	67.53	86.6	96.89	94.39	92.63
3	Denmark	84.42	88.3	92.6	96.44	92.45
4	Australia	66.23	86.9	97.47	85.61	89.99
5	United Kingdom	89.61	79.3	99.54	90.4	89.75
6	Sweden	84.42	79	94.55	95.1	89.55
7	Austria	85.71	83.8	93.89	90.95	89.55
8	Japan	63.64	86.2	97.82	82.29	88.77
9	United States	64.94	85.5	100	80.31	88.6
10	Canada	70.13	79.3	97.67	88.01	88.33

Least Secure Countries

Rank	Country	National Cyber Security Index	Cybersecurity Exposure Index	Global Cybersecurity Index	Cyber Resilience Index	Final Cyber Safety Score
61	Pakistan	41.56	24.5	64.88	79.81	56.4
62	Armenia	35.06	34.5	50.47	82.95	55.97
63	Panama	50.65	43.1	34.11	82.58	53.26
64	Sri Lanka	44.16	25.5	58.65	75.48	53.21
65	Kyrgyzstan	37.66	30.7	49.64	75.62	51.99
66	Ecuador	53.25	34.8	26.3	73.89	45
67	Algeria	33.77	27.9	33.95	67.72	43.19
68	Venezuela	28.57	19.3	27.06	80.1	42.15
69	Honduras	22.08	39.7	2.2	81.83	41.24
70	Bolivia	31.17	21.7	16.14	77.33	38.39

Country Objectives

There are seven national objectives that countries pursue using cyber means. They are:

- Surveilling and Monitoring Domestic Groups;
- Strengthening and Enhancing National Cyber Defences;
- Controlling and Manipulating the Information Environment;
- Foreign Intelligence Collection for National Security;
- Commercial Gain or Enhancing Domestic Industry Growth;
- Destroying or Disabling an Adversary's Infrastructure and Capabilities; and,
- Defining International Cyber Norms and Technical Standards.

Forecast for 2024

Increased AI based threats, met by AI based defence

AI shall drive the next major upgrade in cyber weaponry and will ultimately pioneer the malicious use of AI. AI's fundamental ability to learn and adapt will usher in a new era in which highly-customised and human-mimicking attacks are scalable. 'Offensive AI' – highly sophisticated and malicious attack code – will be able to mutate itself as it learns about its environment, and to expertly compromise systems with minimal chance of detection.

More cyber activity around major events

Big events like the Super Bowl or Olympics creates an increased level of risk for cybersecurity breaches – and not just for the event itself. The game causes a surge on online activity such as search and commerce across industries ranging from entertainment to retail.

Increased cyber operations conducted by nation states

In 2024, we can expect to see an increase in state-sponsored cyberattacks and espionage. These attacks can have significant geopolitical implications and disrupt critical infrastructure. Countries will need to strengthen their cybersecurity defences and work together on international cybersecurity initiatives.

More of Zero Day attacks

A zero-day (0day) exploit is a cyber attack targeting a software vulnerability which is unknown to the software vendor or to antivirus vendors. The attacker spots the software vulnerability before any parties interested in mitigating it, quickly creates an exploit, and uses it for an attack. Such attacks are highly likely to succeed because defences are not in place.

More organizations adopt cybersecurity Outcome-Driven Metrics

The frequency and negative impact of cybersecurity incidents on organizations continues to rise, undermining the confidence of the board and executives in their cybersecurity strategies. Outcome-driven metrics (ODMs) are increasingly being adopted to enable stakeholders to draw a straight line between cybersecurity investment and the delivered protection levels it generates.

Continuous Threat Exposure Management Programs Gain Momentum

CTEM is a pragmatic and systemic approach organizations can use to continually evaluate the accessibility, exposure and exploitability of digital and physical assets. Aligning assessment and remediation scopes with threat vectors or business projects rather than an infrastructure component, highlights vulnerabilities and un-patchable threats.

Identity & Access Management (IAM) to Improve Cybersecurity Outcomes

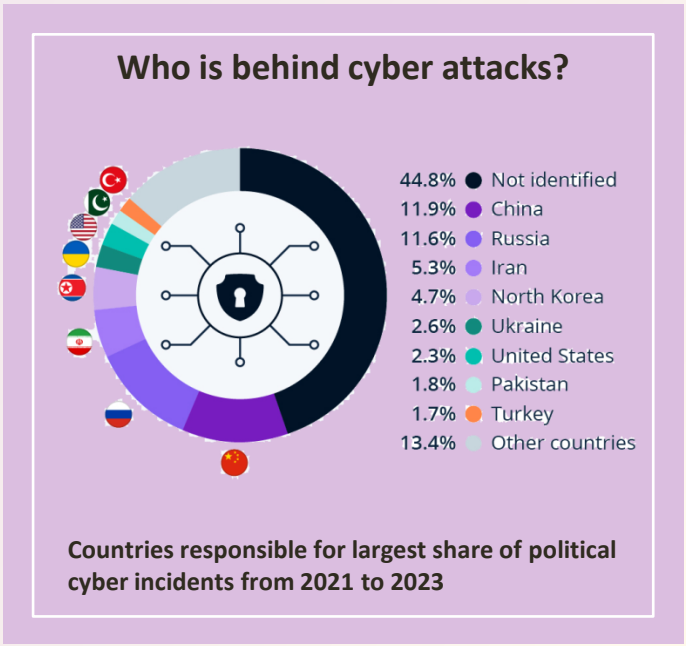
As more organization's move to an identity-first approach to security, the focus shifts from network security and other traditional controls to IAM, making it critical to cybersecurity and business outcomes. While we sees an increased role for IAM in security programs, practices must evolve to focus more on fundamental hygiene and hardening of systems to improve resilience.

Increased Adoption of Zero Trust Cyber Security

The Zero Trust model is all about not trusting any entity within or outside your network. Every user and device, regardless of their location, is treated as a potential threat. This model focuses on identity verification and continuous monitoring to ensure security.

Increasing Threat of Deepfakes

Deepfake technology, which involves manipulating audio and video to create realistic but fabricated content, is a rising concern. Deepfakes can be used for social engineering attacks, impersonating individuals, and spreading disinformation.



Countries responsible for largest share of political cyber incidents from 2021 to 2023

Emerging Challenges

Rising Costs of Cyber Crime

As attack methods become increasingly sophisticated, when these companies are hacked, the costs of rectifying the breach and recovering from downtime can spiral into millions.

The average cost of a cyber breach in 2022 was $4.35 million. It's predicted that cyber crime cost the global economy around $7 trillion in 2022, and this number is expected to rise to $10.5 trillion by 2025.

A concerning statistic is that 67% of SMBs feel that they do not have the in-house skills to deal with data breaches. However, this issue is mitigated as increasing numbers of SMBs are working with Managed Service Providers for cyber security; 89% as of 2022, up from 74% in 2020.

Increasing Attacks on Supply Chain

Supply chains are becoming increasingly interconnected and complex as technology improves. However, this connection presents risks if businesses in the chain aren't adequately protected. Security vulnerabilities in one business can expose partners they are connected with. Cyber criminals are targeting these vulnerabilities, with up to 40% of cyber threats now occurring indirectly through the supply chain.

Research highlights that cyber security leaders are burnt out and in an 'always on' state as increased digital connections demand more of their time. Cyber criminals are using this fatigue to their advantage.

A study has revealed that just 23% of security leaders monitor their partners and vendors in real-time for cyber security risks. These organisations also limit third-party coverage to their immediate vendors and suppliers. This excludes their wider ecosystem of customers, business partners, investors and others.

Internet of Things (IoT) devices at Increased level of risk

The IoT doesn't require human interaction to function, making IoT devices excellent assets in business to automate tedious workflows and reduce the margin for error.

However, these devices are a prime target in cyber crimes. GPS trackers, 'smart' wearables and other IoT devices can hold valuable data but often don't have robust security software.

This was discovered in the case of MiCODUS. The MiCODUS MV720 GPS tracker is a popular automotive tracking device, designed to help with vehicle fleet management. It is hardwired into vehicles, enabling anti-theft, fuel cut-off, geo-fencing and remote control capabilities.

MiCODUS products are used in 169 countries by the general public, government agencies, militaries, law enforcement and businesses. 6 severe vulnerabilities were found in the MV720. Exploiting these vulnerabilities means attackers could track shipments, cut fuel to emergency vehicles or extort ransoms by disabling fleets.

Cyber crime on social media

The growth of social media in recent years has given cyber criminals another avenue of attack. Meta, the parent company of Facebook, uncovered more than 400 malicious iOS and Android apps in 2022 that targeted mobile users to steal their Facebook login credentials.

43% of these apps were 'photo editors', including ones that allowed the user to turn themselves into a cartoon. A further 15% were 'business utility' apps, which claimed to be able to provide hidden features not found in official apps from reputable platforms.

By creating fake reviews, cyber criminals can artificially inflate the ranking of their apps and disguise poor reviews that highlight issues. Unsuspecting users then download the app, where they are then asked to log in using Facebook. The hacker can see any details entered.

Managing the Cyber Future

There are three kinds of responses to cyber threat events:

a. Corrective actions
b. Preventive actions
c. Pre-emptive actions

Since we recognize that corrective actions are expensive, there is a lot of focus on preventive actions through building of systems, awareness, skills, and processes,

Meanwhile, we also realize that almost all cyber threats are intentional acts by human beings, and therefore the best way to fight them is to pre-empt such acts by thinking before someone else do.

Pre-emptive action aims at out-thinking and early-thinking such human intents and establish the preventive systems in place.

Unlike in many other crime scenarios, an advantage that cyber crime has is that it could be simulated without loss of life and property.

Competitions that challenge human thinking like the Cyber Grand Challenge from the likes of MIT, among others establish such platforms where the passionate among rest of humanity can match their wits against possible cyber crimes.

Cost of an average cyber attack is increasing every year, and while preventive systems and actions are an absolute necessity, investing in our pre-emptive thinking goes a long way in improving the preventive methods, and keep the cost and impact of eventual crimes that happen to a minimal level.

Conclusion

The evolving cyber security threat landscape requires organizations and their CISOs to view security through a new, more pragmatic lens. More than ever before, they must balance data security and privacy with the broader objectives of the business.

From a cybersecurity perspective, the impacts of societal, economic, political, and regulatory developments are more consistently felt globally today. The most acute effect of the connected business ecosystem continues to be within global supply chains — for all practical purposes, there are virtually no regions of the world that are isolated anymore.

While new technologies will aid security teams, they can also expand the attack surface. In 2024, the rapidly evolving world of gen AI will provide attackers with new ways to conduct convincing phishing campaigns and information operations at scale. However, defenders will use the same technologies to strengthen detection, response, and attribution of adversaries—and more broadly reduce toil, address threat overload, and close the widening skills gap.

There's a global focus within the cybersecurity universe on compliance in general, with a refined eye toward the overall burden of regulation, as well as the diversity of various reporting requirements.

The cybersecurity landscape is constantly evolving, sometimes in new and unexpected ways. Defenders, often with limited resources, have the monumental task of keeping up.

The Cyber Security Forecast 2024 report from SRIT is our way of helping security professionals prepare for the certainties and uncertainties of the year ahead. We hope our knowledge from the frontlines helps you feel ready.

SRIT India | www.sritindia.com
Established in 1999 | CMMi Level 5
ISO 20000-1:2018 | ISO 27001:2015
ISO 9001:2015 | ISO 14001:2015