Trending Smartphone Device Channel Enterprise CIO Tech DTV Reviews Resources

How Ecommerce is Thriving Beyond Metros Government Push Powers India Toward Unrivaled Tech Leadership Iris Global Delivers ₹100 Crore Worth of Dell and APC Products for Federal Projects ASUS Launches Next-Gen Vivobook 14 F

News

Data Privacy Day: What Tech Leaders Have to Say?

Image Source : www.freepik.com

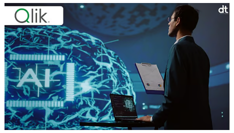
NDM News Network

Published on: 28 Jan 2022, 5:30 am · 17 min read

Related Stories

India's Data Center Capacity to Triple by 2030, Says Avendus Capital Report

NDM News Network · 12 Jul 2025

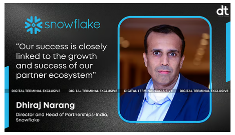


Qlik Empowers Enterprises to Measure Data Trustworthiness with New AI-Focused Trust Score

NDM News Network · 07 Jul 2025

From Chaos to Control: 5 Signs Content Creators and Remote Workers Need NAS

Owais Mohammed · 04 Jul 2025


snowflake
"Our success is closely linked to the growth and success of our partner ecosystem"
Dhiraj Narang
Director and Head of Partnerships India, Snowflake

"Our Goal Is To Make The Snowflake Partner Network The Number One Ecosystem For Data Apps And AI"

Rajeev Ranjan · 13 Jun 2025

Today, data privacy is one of the major concerns for Indian customers. Securing confidential data from internal as well as external threats has become the top priority for organizations that have a huge customer base. Cybercriminals are very active these days and take advantage of the vulnerable security infrastructure for their greed. In these circumstances, organizations don't comply with the data privacy norms and end up being caught by hackers. It sometimes causes them big losses which ultimately creates a bad reputation and legal challenge as well. The government is also proactively working towards providing a safe digital environment to organizations as well as individuals. However, the data protection bill is being delayed which we all are waiting for. On Data Privacy Day 2022, the key leaders from the tech industry have shared their views on why data privacy is important and how it should be taken care of. Read the quotes below.

"Malware, Ransomware And Cyber Threats Have Become More Specialized And Penetrative"

"Data Protection Day serves as a global reminder for one of the most important responsibilities of any organization, which is to keep sensitive and mission-critical data secure. Today, many organizations in India and around the globe are exposed to sophisticated vulnerabilities, as their infrastructure and data security framework is inadequate. Malware, ransomware and cyber threats have become more specialized and penetrative. Once a lapse is identified, attackers can misuse the data and create situations in which data, once lost, may not be recovered. With the hybrid work model, organizations also process complex amounts of data in environments where frequent exchange of data may occur from multiple touchpoints. The influence of emerging tech like cloud-native applications, Kubernetes containers, and AI in day-to-day business activities also increases the risk of misuse of data due to the lapse in the upkeep of cybersecurity goals and IT infrastructure, making organizations vulnerable to cybersecurity threats."

“Consumers are also constantly discovering the information that is collected about them, how that data is used, and how daily breaches put that information at risk. Consequently, organizations must make security a top priority to maintain consumer trust and remain compliant with regulations.

To address these challenges, a few steps that organizations must take, include, an accurate inventory of data. This is critical for adhering to data privacy regulations, such as GDPR. Many organizations may not know the information they have or where it is going, thereby making it difficult to protect it. Additionally, solutions that dynamically allow or deny access based on contextual factors like a user's location, device type, or job function are highly favorable, along with data loss prevention (DLP) capabilities. India is also taking steps to implement a data protection framework that incorporates many elements of the GDPR. Ultimately, in today's highly regulated data environment, Indian organizations need to adopt and build effective compliance strategies to achieve business value. Organizations with low levels of data protection and data governance frameworks need to change quickly.” **- Ripu Bajwa, Director and General Manager, Data Protection Solutions, Dell Technologies, India**

“Data Privacy Day Is The Perfect Time To Evaluate Data Hygiene And Security Protocols”

"Toward the end of 2021, Check Point Research noted that cyber-attacks against corporate networks had increased by a staggering 50% on the previous year. The education and research sector was the hardest hit, averaging 1,605 attacks per week, with government organizations, communications companies, and internet service providers close behind. Even attacks on the healthcare sector were up 71% on pre-pandemic levels, showing nothing is off-limits to threat actors. In our 2022 Security Report, we also noted that email had become an increasingly popular vector for distributing malware throughout the pandemic, now accounting for 84% of malware distribution. Beyond the corporate world, it was also clear that large-scale attacks on critical infrastructure, such as the Colonial Pipeline incident, had a very real impact on people's day-to-day lives, even threatening their physical sense of security. Data Privacy Day, or Data Protection Day as it's known in Europe, is the perfect time for individuals and businesses to evaluate their data hygiene and security protocols to ensure their data is kept as safe and secure as possible."

"Check Point Software is beginning 2022 with a new strategic direction that follows the mantra: You Deserve the Best Security. While adopting the kind of best security practices promoted by Data Privacy Day is vital, it's only a baseline. We know that businesses can't afford to settle for second best when it comes to defending themselves in a constantly evolving threat landscape. That's why we're working hard on cutting-edge technologies such as our recently announced Quantum Lightspeed firewalls, and why each and every one of our software solutions are powered by our global real-time threat intelligence platform." **- Sundar Balasubramanian, Managing Director, India, and SAARC, Check Point Software Technologies**

"Data Protection Is Only Successful When All Components Within The Infrastructure Are Prepared To Handle It"

"As the union government gears up to introduce laws to protect consumer data, organisations should bear the onus of educating their employees. Data protection is only successful when all components within the infrastructure—including all employees—are prepared to handle it. To do this efficiently, data protection must be built right from the design stages of all services and operations. It should be present as a strong, invisible layer. It is best to educate employees on the do's and don'ts of data protection in a way that is contextually integrated into their work, as opposed to relying solely on periodic trainings. Given the forthcoming legislation, corporate data management is more important than ever, and it's up to business leaders to create the teams, structures, and expertise to keep all their corporate data well-protected and staying compliant in 2022." **- Rajesh Ganesan, Vice President, ManageEngine**

“Data Protection Is All About Freeing Ourselves From Digital Slavery”

“It's time to understand what freedom means, mainly digital freedom. We leave our digital trails whenever we engage digitally. Algorithms have started using the data to condition our minds, influence, and sometimes even dictate what we should be doing in the future. Data protection is all about freeing ourselves from digital slavery. The goal of data protection is to give power to the data owner. It is the capacity to decide what data should be stored, how it should be used or not used, and to make sure they don't end up as slaves to the machines. Data protection means empowerment to the consumer so that they have the freedom of choice every time they shop. It is about establishing a level playing field and healthy competition in business. Most importantly offer a guarantee about the security and safety of personal and business data. On this data protection day, let us commit ourselves to understanding our rights to enjoy our freedom as digital citizens.” **- Kumar Vembu, CEO and Founder, GOFRUGAL**

“This Data Privacy Day We Highlight How We Can Better Protect The Data”

"Software Bots Have Sharing Issues Too

It's not just humans that are susceptible to clicking on the wrong link or are perhaps a little too cavalier about what they share about themselves. Software bots have sharing issues too, and this Data Privacy Day we highlight how we can better protect the data that they access from being exposed. Software bots – little pieces of code that do repetitive tasks – exist in huge numbers in organizations around the world, in banking, government and all other major verticals. The idea behind them is they free up human staff to work on business-critical, cognitive, and creative work, but also helping improve efficiency, accuracy, agility, and scalability. They are a major component of digital business. The privacy problem arises when you start to think about what these bots need so they can do what they do. Much of the time it's access: If they gather together sensitive and personal medical data to help doctors make informed clinical predictions, they need access to it. If they need to process customer data stored on a public cloud server or a web portal, they need to get to it. We've seen the problems that can arise when humans get compromised and the same can happen to bots – and at scale. If bots are configured and coded badly, so they can access more data than they need to, the output might be leaking that data to places where it shouldn't be. Likewise, we hear about insider attacks and humans being compromised to get to sensitive data virtually every day. Machines have the exact same security issues; if they can access sensitive data and they aren't being secured properly, that's an open door for attackers – one that can put individuals' privacy at risk. Attackers don't target humans to get to data, they just target the data. If machines, especially those in charge of automated processes (think repeatable tasks like bank transfers, scraping web data and moving customer data files) provide the best path to get to the sensitive data, that's the one the attackers will choose."

"BYOD, The Sequel: Your Privacy at Risk

One of the many, many ways that life has changed for several of us in the last couple of years is the hybrid work phenomenon. On the plus side, we are supporting our local coffee shops and saving money on the commute. On the minus side, we don't get to see our colleagues and we wear jogging bottoms every day. Oh, and we're causing data privacy issues for our employers and their customers. The roots of this are buried in the sudden change of environment that many companies had to provide for. Security policies were written on the assumption that there are premises; people would work in a restricted access area or room. They would have workstations that were company-provided and up to date with easily enforceable security policies. Covid spurred many privacy issues here. Many workers were given a budget and told to avail themselves of a laptop. These will not have the same level of security as one that your employer gives you, or as your office workstation. Likewise, the concept of secure work areas at home is not a realistic one for most of us, with families, flat mates, or strangers in the coffee shop peering over our shoulders. The hybrid work model has changed the privacy game as well. It means that companies have to re-evaluate how data privacy is enforced in 2022. Securing access to sensitive data by remote employees will be big in 2022." **- Sumit Srivastava, Solutions Engineering Manager – India, CyberArk**

"People Are More Empowered Than Ever To Exercise Their Rights And Reclaim Control Of Their Information"

"Data privacy reform has changed our global community forever. As we begin 2022, organisations face an emboldened world demanding greater accountability and trustworthiness. The recent steps taken by several countries to bolster their consumer privacy rights and processing activities (such as China's Personal Information Protection Law) will have a far-reaching global impact on privacy rights and data protection practices. People are more empowered than ever to exercise their rights, submit Subject Rights Requests (SRRs) and reclaim control of their information. They want to understand how their data is used and to access, correct, delete, and restrict use. To meet these data-intensive demands and overcome a scarcity of resources to support key business activities, organisations must embrace process automation for SRR response and apply case management tools that best track its performance and effectiveness. A well-executed program that delivers a strong experience will be critical to improve customer satisfaction and loyalty." **- Andy Teichholz, Global Industry Strategist, Compliance & Legal, OpenText**

"It Is Critical For Businesses To Be Able To Manage All Devices That Access Their Network"

Data privacy concerns have been exacerbated by the pandemic as we have seen an uptick of ransomware and cybercrimes with bad actors taking advantage of the rapid shift to remote work, the increase in online deliveries and the proliferation of QR codes. The sheer amount of data we share about ourselves online is a privacy concern and more alarming is that many workers are using the same devices for personal and business activities. For this reason, it is critical for businesses to be able to manage all devices that access their network, along with effectively prioritizing and remediating vulnerabilities that pose the most danger to their organization.

The Ransomware Spotlight Year End report released earlier this week underscores the need for organizations to address the rapidly evolving threat landscape, with a 29% increase in the number of vulnerabilities tied to ransomware and a 25% increase in ransomware families the frequency and sophistication of cyberattacks that will only escalate.

At Ivanti we continue to innovate and lock arms with our customers to help enable and secure the Everywhere Workplace. For instance, with Ivanti Neurons for Patch Management, which came out of beta a few days ago, we automate patch management for our customers and help them identify and patch their most critical vulnerabilities proactively. This is critical as a recent study that we conducted revealed that 71% of IT and security professionals found patching to be overly complex and time consuming. It is critical for businesses to have real-time intelligence on known exploits along with threat context for vulnerabilities so they can respond with more agility to the vulnerabilities that place their organization at the greatest risk.” **- Lana Xaochay, Data Privacy Officer, Ivanti**

"Data Privacy Has Become a High Priority for Corporations Across India"

“Data privacy has become a high priority for corporations across India, owing to factors such as increased global business operations and outsourcing of work to specialists outside of the organisation. Furthermore, the increased adoption of hybrid working models has made data maintenance and security more difficult. The significant increase in digital convergence has made it possible to easily exploit data beyond the stated intentions. This has added additional responsibility on organizations to protect the personal data of its employees and customers. Gartner predicts that by 2024, worldwide privacy-driven spending on data protection and compliance technology will exceed USD 15 billion annually. The Indian Government too has proposed a data protection law for data privacy assurance to support the ongoing issue around data privacy breaches. These standards seek to provide a privacy assurance framework for organizations to establish, implement, maintain and continually improve their data privacy management system.” - **Sandeep Bhambure, Vice President & Managing Director, Veeam India & SAARC**

"Data Privacy Day Should Serve as a Catalyst in the Fight Against Rising Cyber Threats"

“As we increasingly blur the line between our online and offline lives, Data Privacy Day is the little reminder we need at the start of each new year to ensure our personal information is protected. Even though we live in a digital world, we are often not fully cognizant of data privacy until our data has been compromised.

Data is one of the most important assets for organizations. Thus, data privacy and security take center stage in their cybersecurity strategy. To enable seamless business recovery and develop a safe post-Covid data-centric economy, organizations need to move beyond just basic compliance measures to achieve continuous situational awareness for faster threat detection and response. This year’s Data Privacy Day should serve as a catalyst in the fight against rising cyber threats and bring greater attention toward protecting the critical data of businesses. Collaborative cyber defense, threat intelligence sharing, and data protection strategies must be leveraged to empower governments and private organizations in mitigating cyberattacks. More emphasis should be placed on implementing secure authentication mechanisms to minimize the risk of credential compromise, while ensuring secure and easy access for all stakeholders.

In the age of the work-from-anywhere economy, business leaders should realign their security priorities to manage risks affecting sensitive information. In order to guarantee a seamless flow of data from endpoints to cloud-based services and data centers, it is becoming more important to protect the data in transit as well. Crucial business data in India can be protected through investment in the modernisation of security infrastructure, using secured collaboration and information-sharing platforms, leveraging threat intelligence for proactive cyber defense, using security orchestration and automation (SOAR) to streamline SecOps, and performing periodic security and risk assessments. Individuals must take control of their digital footprints and privacy as we continue to telecommute in 2022. Moving forward, cyber situational awareness and hygiene will continue to play a key role as one of the pillars of data privacy.” **- Akshat Jain, CTO & Co-Founder, Cyware**

“Cybersecurity Vulnerabilities Continue To Increase As Companies Grow Their Digital Footprints”

“In recent years, data privacy compliance has become a critical consideration driving critical business decisions as companies look to digitally transform. Cybersecurity vulnerabilities continue to increase as companies grow their digital footprints due to the massive amounts of data being generated. The Data Privacy Day comes as a reminder for organizations to assess their cyber risks and ensure strong data privacy protections are in place but in such a way that will not impede innovation within the digital economy. Due to the increasing complexity of data flows, enterprises need to evolve past securing data at rest to a posture of continuous governance where all data is protected.

Increasingly, we are seeing enterprises place, manage and analyze data at the edge, closer to their users, services and clouds. Meanwhile, concerns over the security and privacy of data in movement and/or in the cloud have also increased. This situation is more critical in Asia-Pacific and has driven the need for better technology and infrastructure solutions that improve data accessibility, security and control, while also meeting increasing data privacy requirements. It is a balancing act.

At Equinix, we support many of the largest enterprises in the world. Through our Equinix Privacy Office, we proactively manage our own compliance with applicable new and evolving data privacy laws and seek to assist customers to do the same. Our data security practices and controls around our own global platform of systems and processes are robust. Our digital services like Network Edge and a rich set of security-focused partners in our ecosystem, which sets up these security services closer to the user to protect that data locally. Our goal is to embed the concept of privacy by design into new system deployments and business process improvements across various aspects of our business, as well as offer our clients systems and infrastructure they can rely on.” - **Peter Waters, Chief Privacy Officer, Equinix.**

“Data Protection And Security Have Become Core To Businesses”

“Data used to be a by-product of business. Every organisation business recorded transactions, stored product, process, customer records, during the normal course of conducting business. The sea change in the past few years, is that with deep tech, vast amounts of telemetry, AI, ML, analytics, businesses are being built on data. Data is creating value. Data is the business. Data is the source of competitive advantage. Data also gives rise to risks involved. In addition to traditional risks, there are also the ongoing risks of ransomware, denial of service (DoS) and, theft of intellectual property. No wonder, data protection and security have become core to businesses.”

“Beyond the headline-grabbing numbers, there remain core principles sensible organiszations must observe. Above all else, good security management is predicated on good data management. Along every step of the security journey – from prevent to detect to respond – knowing where your data is, how to extract it, and how it interoperates across and beyond organizsational boundaries are key to ensuring you protect yours and your customers’ most valuable intelligence. With data privacy regulations and requirements growing more complex, users must look at solutions that simplify compliance in encryption and sophisticated AI that maps and classifies data.” **- Ravi Chhabria, Managing Director, NetApp India**

“Cloud Security Has Been Voted As One Of The Biggest Security Threats That Organizations Face”

"With the new normal dictating the ways of our lives, businesses have turned to digital transformation to ensure productivity and continuity. Cloud has emerged as the biggest enabler by fueling both remote and hybrid work infrastructure. Hence, we had seen Microsoft claiming, just a few months through the pandemic that they have witnessed two years of digital transformation in two months as its customers started adopting cloud solutions. According to Gartner, in the aftermath of the pandemic, the worldwide end-user spending on public cloud services grew by 18.4% in 2021 to a total of USD304.9 billion."

"Although a great enabler, cloud raises a lot of security challenges. Cloud security has been voted as one of the biggest security threats that organizations face. Enterprises often misunderstand cloud security as the sole responsibility of the cloud services provider as against viewing it as a shared responsibility. Robust cloud security provides multiple levels of controls within the network infrastructure for the protection of cloud-based assets. Whether in a public or private cloud, enterprise need access to security tools that can protect their data and resources from theft, leak, or natural disasters. One more important aspect that cannot be ignored when it comes to security is the 'Human Error'. Surprisingly enough, it is the most neglected link in cybersecurity. Human error in cybersecurity breach is an age-old problem. For years, it has consistently been identified as a major contributing factor to data breaches. The average cost of data breaches from human error stands at USD3.33 million, according to IBM's Cost of a Data Breach Report 2020."

"It doesn't matter how many security measures and precautions an organization undertakes, a simple human error can still put everything in jeopardy. Whether users are negligent, careless, or simply uninformed, a human error can lead to a cyber-attack and thereby data breach. Hence, enterprises along with cloud service providers need to develop detailed and stringent security policies that clearly outline access and privileged access management, zero trust policy, user activity monitoring, and further educate their employees on the negative impact of cyber-attacks and positive impact of best practices. Security shouldn't be treated as an isolated activity. It is a shared responsibility right from the management to vendors to even the new entrants in an organization. Hence, an organization can consider itself completely secure against breaches only by aligning all its stakeholders towards the common goal of ensuring comprehensive security.” **- Neelesh Kripalani, Chief Technology Officer, Clover Infotech**

“It Is Imperative To Have A Re-Architecture Of The Cyber Strategy”

“Over the last 2 years, there has been a significant rise in cyber-attacks all over the world. The pandemic has increased our dependency on mobile devices and remote access to core business functions. While remote working became the saviour, it also introduced a new set of security challenges by raising concerns regarding identity-based threats, privacy breaches and the loss of essential data from unprotected devices and systems. Despite the best efforts of security teams, attackers consistently took advantage of vulnerabilities, discovering new ways of infiltration and taking advantage of people’s curiosity as well as their fears around Covid, leveraging socially engineered lure files and tactics.

There is a huge digital shift that has been created by the pandemic where many industry sectors have witnessed an accelerated approach towards digital transformation and their erstwhile perimeter has moved beyond their enterprise firewalls to cloud; either a public cloud, hybrid cloud or a private cloud. This has added complexity to the IT architecture stack and also increased the potential attack surface for adversaries to exploit; and often under-resourced security teams to protect. Today’s new perimeter needs to be buttoned up with operations and security collaborating to create a secure network. With more data moving to the cloud every day, it is imperative to have a re-architecture of the cyber strategy which should go around all three dimensions of security i.e. people, process and technology.

While many cloud service providers offer basic levels of data security, it is critical for organizations to develop and implement a comprehensive data security strategy that’s scalable and combines automation with human threat hunting and threat intelligence. Another critical element of a data security strategy is real-time monitoring, detection and response. These threat detection and response capabilities should be supported by machine learning and analytics to better identify anomalies and malicious activity.

Companies require proficient and skilled cyber security experts who can keep their endpoints, cloud workloads, identify and data secure. Unfortunately some organizations still rely on legacy security solutions that are just not fit for purpose especially as adversaries evolve their tools, techniques and procedures (TTPs). They need security that is scalable, built for the cloud and can carry the same level of control and visibility from their on-premises environment into remote working environments. Meeting these challenges head on with a layered, unified approach to security will enable organizations to move forward with their cloud plans with the knowledge that their users and data are well guarded.” **- Nitin Varma, Managing Director, India & SAARC, CrowdStrike**