VIEW POINT

SECURITY & PRIVACY, COMRADES IN PROTECTION – THE PAST, PRESENT AND FUTURE

Infosys®
Navigate your next

Introduction

Security and privacy domains have had distinct journeys so far, starting from their origins through the evolution over time. However, a force multiplier in the potential for success can be decision makers and practitioners from these domains complementing and respecting each other's perspectives in strategizing and operating collaboratively, towards a common goal in protecting the interests of a diverse spectrum of stakeholders in the ecosystem.

Such a multi-disciplinary approach has accelerated the convergence and increased interdependencies in the evolving landscape of regulations and standards across nations, states, industries, as well as people, process, tools and technologies especially - AI/ML, IoT and bigdata/ analytics. So does the wider adoption of both security and privacy practices thus being embedded as part of organizational cultures by design.

While we compare further across security and privacy in this paper, the way forward looks promising and mutually beneficial as the borders get blurred and avenues for collaboration expand.

1. The histories of security and privacy

Merriam-Webster dictionary defines security as "The quality or state of being secure such as freedom from danger, fear or anxiety" OR "measures taken to guard against espionage or sabotage, crime, attack, or escape".

The idea of securing people and property dates back to the ancient Egyptian Pharaohs or to ancient Rome. Data security is said to have started with them leveraging encryption to protect sensitive information - e.g., in military by shifting letters in a document's message. The more modern way of security seems to have evolved from the 19th century, with many advancements in tools/ processes/technologies on the way, including IT/cybersecurity evolution post internet gaining popularity (along with the related threats too) from the 20th century.

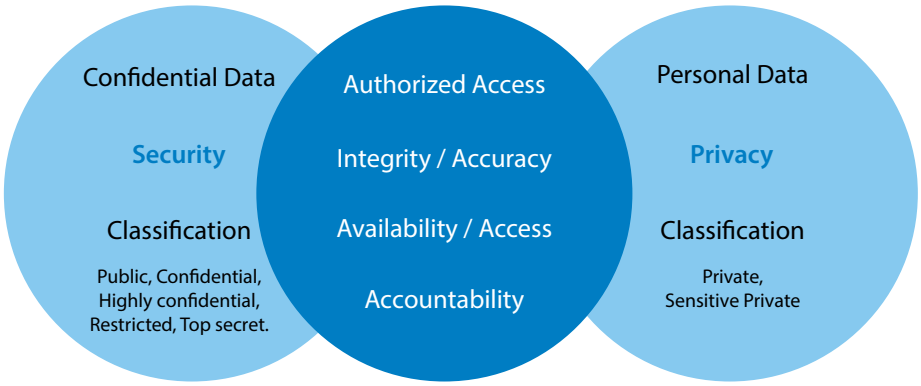
With regards to privacy, Merriam-Webster defines it as "Freedom from unauthorized intrusion". And IAPP defines it as the "Right to be let alone or freedom from interference or intrusion", "right to have some control over how your personal information is collected and used" etc.

Privacy has its roots in more nuanced human rights movements across the globe (especially the US and Europe) culminating in the Universal Declaration of Human Rights under the UN auspices in 1948 – this continues as the base inspiration and reference for most privacy regulations worldwide, including the most popular one viz. GDPR.

Thus, while security comes from the perspective of protecting assets of a nation or an organization, privacy looks through the prism of protecting personal rights and liberties.

2. Comparing and contrasting

Below is a simple representation of how data security and data privacy compare – the key point being that neither all confidential data is personal nor vice-versa. This is also reflected in the different data classification methods applicable.



While privacy cannot be achieved without security, the reverse need not be true - having a robust security program doesn't necessarily guarantee adequate privacy (though will serve as a good foundation to work on).

Thus, privacy brings in extensions/ nuances of the CIA triad, focused more on personal rights/liberties – much beyond enterprise business/security goals or national security requirements. This at times leads to divergent perspectives and even friction among the stakeholders involved – needing balancing between organizational interests and individual interests, without extreme positions leading to one compromising the other. Some key cases in point are as follows – this calls for the related stakeholders (law makers, regulators, practitioners, lawyers, individuals etc.) to acknowledge this and make necessary amends balancing across multiple perspectives.

a) Monitoring – for security practitioners, this is a key function to proactively 'detect' any anomalies ahead of time and 'defend' the organization data/assets from security threats. Individuals being the weakest link, this often involves controlled tracking of user actions and behavioral patterns, leveraging UEBA or otherwise. Whereas privacy practitioners could perceive this as an intrusion of individual privacy rights, thus conflicting with the organizational security interests.

b) Data management strategy – there can be multiple data elements (especially of employees) that an organization collects, stores, processes or deletes during the course of employment or later, as per applicable rules and regulations (as well as financial and security interests). There can be multiple schools of thought on the adequate/appropriate types/ depth of data management which is needed for this. E.g. Extreme positions of Work Councils on this could potentially create impediments in organizational operations (including security).

c) HR actions – every process driven organization (irrespective of the size, scale, industry, or geography) would have documented employee policies and procedures, and consequence management steps listed against any deviations (including related to security). The analysis and decision making around this would include processing of multiple personal data elements as necessary and could potentially be objected to by the employee (or Work Councils), from the perspective of privacy rights.

3. Regulatory landscape

Let's try to compare ISO27001 (a certifiable global security standard) and GDPR (a global privacy regulation with no certification provision yet). Both follow a risk-based approach to protection through controls aimed at bringing residual risks to an acceptable level. While ISO27001 sees encryption from BCP/DR perspective, same could be leveraged to protect personal data in GDPR. The ISO27001 requirements of risk assessment and asset management would greatly benefit as controls towards GDPR expectations on DPIA and data accuracy/ storage. While GDPR expects implementing appropriate technical and organizational measures to achieve the privacy objectives, it doesn't elaborate adequately on the nuts-n-bolts (the "how" part) – this mostly involves security controls, and hence practitioners end up following guidance from security standards/regulations for the best practices.

ISO27701 has been a standard aimed at PIMS (Personal Information Management System) effectively as an extension of ISO27001, to complement it for the privacy aspects.

4. Security and privacy by design

A key factor in assuring adequate protection of information assets of any organization is to have both security and privacy embedded by design (and default). Any reactive measures as afterthought can have only limited outcomes and predictability.

All stakeholders need to be brought on board regarding the related criticality and the need for prioritization. This is often achieved through education, training, certification as well as appropriate policies and processes / procedures, backed by leadership support as well as deterrent/ penalty measures as applicable.

While there are various frameworks and methodologies available for SbD and PbD separately, the 32 Security & Privacy by Design Principles (S|P) principles from the Secure Controls Framework (SCF), is a free resource for businesses to help ensure that both security and privacy practices are implemented by design and by default. With a comprehensive listing of over 1,000 cybersecurity and privacy controls, this is categorized into 32 domains that are mapped to over 100 statutory, regulatory, and contractual frameworks, also keeping in mind the industry best practices.

5. Complementing role in enterprise strategy, objectives and operations

Privacy has come a long way from a political/abstract concept driven by human rights activists to a specialized function where the risks to businesses are substantially high, leading to evolution of a matured ecosystem including increased awareness, comprehensive regulations/standards with clear accountabilities and deterrents/penal actions listed out, and a specialized pool of practitioners who have a hybrid expertise from legal, privacy and security domains.

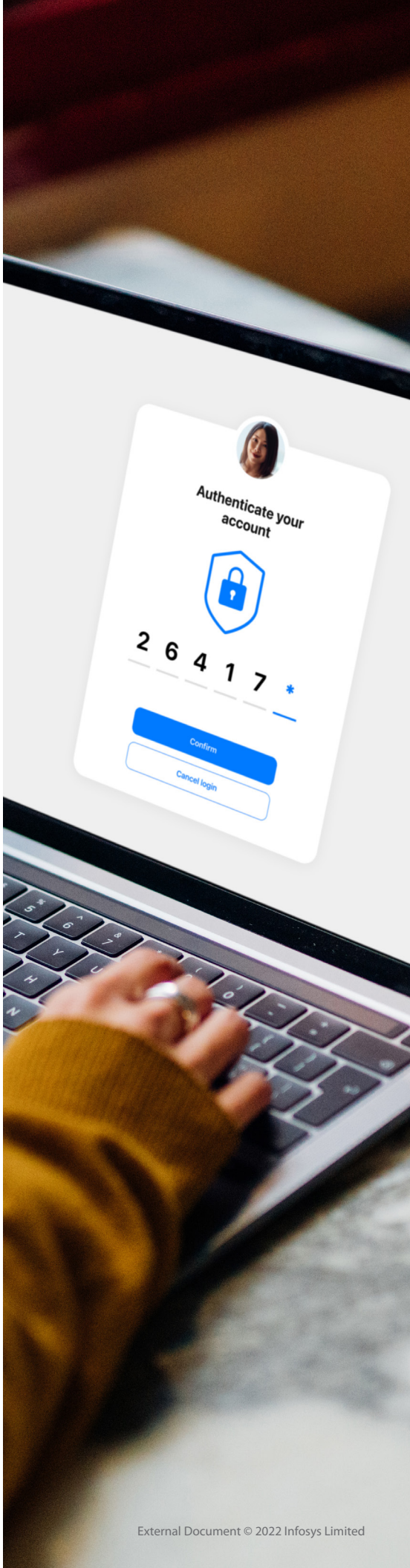
Both security and privacy have been integral part of ESG considerations, and cost of breaches is becoming exponentially high. This has prompted organizations/businesses to co-opt privacy as a top enterprise risk and key value-adding differentiator, thus having a place on the table for strategy design. This aids in optimally and effectively achieving business objectives while balancing out different perspectives and stakeholder interests, with an eye also on protecting their reputation, brand value as well as market share – which are directly linked to the customer trust on (especially their data) being in safe hands – a journey security went through around a decade back. This gets compounded by the dynamic ecosystem of tools, technologies, and maturing regulatory landscape.

While privacy can define and govern adherence to certain norms to protect individual rights, need support from security controls to accomplish them. For most organizations with operations spread large enough to have a structured governance in place, enterprise strategy and objectives should consider perspectives from both security and privacy. For them, adherence to security standards/ regulations sets a base for ensuring compliance to privacy regulations as well, with additional privacy controls as a cherry on the top. Hence organizations could design a unified control framework covering all the applicable security and privacy regulations, with a minimal global/enterprise baseline and additional customization for specific geos and functions as necessary.

There is ample scope for security and privacy teams to collaborate leveraging the synergies, complementing each other and being aware of additional perspectives while prioritizing initiatives, making choices/decisions on processes/ procedures/tools/technologies etc. While it's highly advisable to follow this approach in day-to-day operations to improve efficiency and effectiveness, it's a must have during a crisis/breach situation as it's a race against time, trying to beat the adversary and restore/ recover business operations.

Some areas of collaboration could be as follows:

- Joint operations in risk management – both in "peace" times and "war" times (breach war rooms)
- Cross utilizing impact/risk assessments and data inventory/ classifications
- Joint review of policies/procedures - including but not limited to AUP, third party management, hardening, data encryption/retention, monitoring etc., with additional focus on potential areas of friction if looked at in isolation
- Holistic view in (integrated) user trainings
- Governance framework for ongoing communication and collaboration, with clear escalation paths to manage potential conflicts



6. Evolving ecosystem - People, process, technology / tools

People are an asset and the weakest link while protecting security or privacy in any organization. Privacy being a relatively new and continuously evolving discipline, there is an acute demand-supply gap in skills and competency in the market. Hence, it's important for organizations to hire, nurture/reskill and retain the right talent to ensure continuity and optimized risks for the enterprise. Being a hybrid discipline (across legal/human rights, privacy, and security domains), (one-time and ongoing) training programs and certifications do help build the foundation with a holistic perspective, bolstered further by hands-on experiences.

The maturity of any organization, and the predictability of any desired outcomes, is often highly dependent on the policies, processes, procedures they define and enforce – even with the right funding and talent brought in. Not only these need to be designed considering the applicable risks and ecosystem of the organization, but they also need to be continuously updated as needed. The myriad of regulations, standards, and guidelines available, including guidance from regulators and government bodies, do serve as pointers to align and enrich the documentation.

Like in other fields, tools, and accelerators (especially PETs / Privacy Enhancing Technologies) do help serving privacy interests of data subjects and organizations better. As these evolve over time, with overlaps between security and privacy, procurement and deployment decisions are better driven jointly by both teams to improve efficiencies, contextualized based on the scale, spread, domain, business model, and overall ecosystem of the organization.

7. Emerging trends and the way forward

As per Perkins Coie 2022 report, data privacy and security are key emerging technology areas along with AI, ML, digital media, green tech and healthcare technology. Some emerging areas in privacy and security include synthetic data, cryptography, hacking strategies, differential privacy, data resilience, quantum computing and blockchain.

Organizations increasingly utilize data analytics and big data to have a competitive edge especially with several zettabytes of data getting processed every year globally as the economy grows. However, that also increases their responsibility to create and retain trust through protecting the data, have high level of transparency at all stages etc., as new data security risks emerge, with digitization helping accelerate new business models and ways of working.

Conclusion

With regulations and standards getting firmed up and strengthened across the globe, there is an increased focus on and attention to privacy aspects (along with security) by nations and organizations at a much higher strategic level, than limited to personal rights/liberties. And with commitments on both security and privacy forming key components of ESG considerations, enterprises (and their boards) are increasingly expected by the stakeholders to ensure compliance for the larger good of society and being good corporate citizens.

In this backdrop, we can expect the convergence and collaboration between security and privacy disciplines to further accelerate, as a force multiplier in the potential for success, when practitioners from these domains do complement/respect each other's perspectives in strategizing and operating collaboratively, towards a common goal in protecting the interests of diverse spectrum of stakeholders in the ecosystem.

With Infosys CyberSecurity, our clients have Digital-trust. Assured. And throughout the journey towards further enhancing cybersecurity maturity, we advise our customers on best practices to balance across diverse perspectives as stated in this article.

Hundreds of our clients including Fortune 500 companies (across geos and industries) have entrusted the security management of their critical systems with us and would bear testimony to our capabilities and delivery excellence.

About the Authors

Vishal Salvi

CISO and Head of CyberSecurity Practice

Vishal Salvi has over 27+ years of experience in cybersecurity and information technology across different industries. He has extensive management and domain experience in driving transformational cybersecurity programs, engineering and sales. He is a well-known leader in the cybersecurity industry within India as well as globally and has been part of the cybersecurity domain for the past two decades. He is a regular speaker in major local and global cybersecurity conferences. Vishal is also a member of various advisory councils and boards that provides leadership and direction on various cybersecurity frameworks and standards to drive adoption of cybersecurity across the industry. Vishal holds a degree in Computer Science Engineering and MBA in Finance. His certifications include CISM and DSCI Certified Privacy Professional. He has received numerous awards from prestigious institutions such as DSCI, CSO Forum, ISACA etc.

Oommen Thomas

Group Project Manager

Oommen Thomas manages key strategic initiatives for the Cyber Security Practice at Infosys, including managing GTM strategies of industry leading offerings and optimal business aligned solutions for global customers. He is an enthusiast on innovations in the CyberSecurity, Governance Risk and Compliance, and Data Privacy domains, and has been actively associated with security/privacy/management communities including through forums like ISACA, IAPP and PMI. A continuous learner with around 3 decades of IT industry experience handling multiple domains, roles, and functions, Oommen has been certified in CGEIT, CRISC, CISM, CSX-P, CPISI, ISO27001-LA, DP/GDPR-LI, CIPP/E, CIPM, TOGAF, PMP and ITIL. He volunteers for IAPP as Co-Chair for the Pune Chapter and serves on their Diversity in Privacy Advisory Board.

References

1. https://www.vodafone.com/business/news-and-insights/blog/gigabit-thinking/a-brief-history-of-security#:~:text=Or%20to%20
2. https://safecomputing.umich.edu/privacy/history-of-privacy-timeline
3. https://en.wikipedia.org/wiki/Privacy
4. https://reciprocity.com/difference-between-gdpr-and-iso-27001/
5. https://dataprivacyparty.com/?p=1359
6. https://www.perkinscoie.com/en/emerging-technology-trends.html
7. https://www.securecontrolsframework.com/security-privacy-design-principles

CyberSecurity@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next