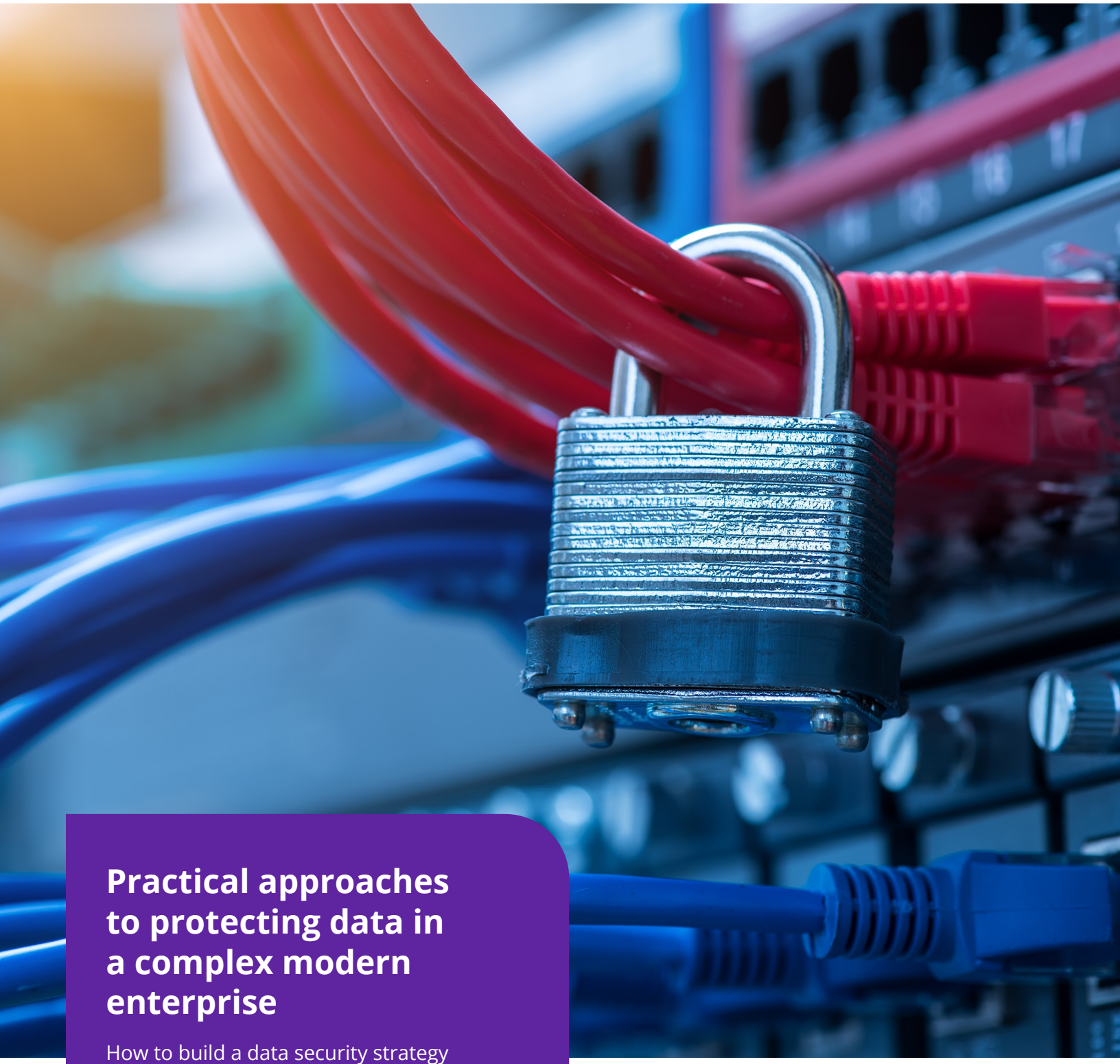
DXC TECHNOLOGY



Practical approaches to protecting data in a complex modern enterprise

How to build a data security strategy that supports real-world business needs in an era of AI, cloud, cyberthreats and privacy concerns

New threats to data protection

Strategic management of information capital is a fundamental competitive advantage that is becoming more important by the day. The overall big data market is expected to grow at an 11 percent compound annual growth rate to $103 billion by 2027.

By 2030, it is anticipated that powerful cloud-based data mining solutions will be accessible to every business — from large enterprises to small, family-owned operations.[1] Companies can leverage this increasing scope and volume of data to drive innovation, enhance business intelligence, optimize processes, improve the customer experience, boost productivity and identify operational efficiencies.[2]

As the adage goes, "With great power comes great responsibility." The commoditization of data has led to privacy concerns and regulatory change.

While the shift toward maximizing data usage and digitizing business processes has benefits, it can also increase an organization's exposure to unintentional or malicious actions, and impact the confidentiality, integrity and availability of electronic data assets. At the same time, social norms and consumer attitudes are becoming increasingly intolerant of privacy violations, so enhancing customer engagement through data-driven insights now needs to be coupled with maintaining consumer trust. An effective data protection and governance regime aligned to an organization's overall objectives will help reduce risk and enable business success.

This paper describes key elements underlying several best practices and approaches to data protection. These include linking some fundamental security methodologies to data protection processes in order to build a data security strategy that truly supports an organization's risk appetite and security requirements.

Implementing that strategy requires effective processes, resources and tools. When resources and budgets are limited and markets are tough, prioritizing and using these resources efficiently becomes even more important. With that in mind, organizations need to implement a governance framework that supports managing data as an asset with the same diligence they use to manage other assets.

Trends impacting data protection requirements

Legal and regulatory trends — including privacy issues — and the evolving cyberthreat landscape are shaping data protection requirements.

Legal and regulatory environment

As the adage goes, "With great power comes great responsibility." The commoditization of data has led to privacy concerns and regulatory change. More data protection and privacy laws have been adopted globally, and financial penalties for noncompliance have increased. These laws and regulations have led to inconsistencies in mandated requirements and questions about how they apply to specific types of data, organizations and geographical locations.

[1] Kobielus, James (2018). "Wikibon's 2018 Big Data Analytics Trends and Forecast," Wikibon. https://wikibon.com/wikibons-2018-big-data-analytics-trends-forecast/

[2] Fosso Wamba, S., Akter, S., Edwards, A., Chopin, G. and Gnanzou, D. (2015). "How 'big data' can make a big impact: Findings from a systematic review and a longitudinal case study," International Journal of Production Economics. doi:10.1016/j.ijpe.2014.12.031

Taking a more proactive approach to data protection and adopting architectural principles that cater to changes in the legal and regulatory landscape can help enterprises remain competitive and minimize future compliance costs.

Gartner predicts that by 2023, "65 percent of the world's population will have its personal information covered under modern privacy regulations," compared to only 10 percent in 2020.[3] Organizations must shape their data protection regimens to comply with one or more country-specific data protection and privacy laws and regulations. Failing to comply puts organizations in the crosshairs of regulators and can lead to substantial fines, as demonstrated by recent high-profile data breaches.[4,5] The European Union's (EU's) General Data Protection Regulation (GDPR) introduced in 2018, the Australian Notifiable Data Breaches (NDB) scheme, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act of 2018 (CCPA) and many other laws and regulations from Asia to the Americas are complex to comprehend and implement — especially for corporations operating in multiple countries with conflicting laws and regulations.

One approach is to establish an enterprise-wide data governance strategy that can be adopted and customized to suit local laws. Taking a more proactive approach to data protection and adopting architectural principles that cater to changes in the legal and regulatory landscape can help enterprises remain competitive and minimize future compliance costs. The strategic management of information capital — avoiding investments in technology and investments that must be drastically changed later to comply — requires keeping an eye on evolving data protection and privacy requirements. This could mean, for example, preemptively pseudonymizing data in anticipation of potential legal requirements.

Cyberthreat landscape

While most malicious attacks are financially motivated, designed to obtain funds through deception or coercion, they also have broader consequences for an organization's data protection obligations.[6] The evolving cyberthreat landscape is influencing data protection requirements in two significant ways.

First, financially motivated email account compromise schemes are indirectly causing data breaches. A fraudster with email account credentials can access everything in the compromised account's mailbox, plus, those same credentials could expose cloud storage or other data repositories.

Second, some ransomware operators are now using dual extortion tactics to profit from malicious activity by taking advantage of the fines associated with breaching data protection laws. The bad actors steal sensitive data before the files are encrypted and then threaten to publicly disclose this information if the organization refuses to pay a ransom fee. To incentivize payment, the ransom demanded is usually less than the anticipated fine and the costs of recovery from the attack.[7]

Validating exfiltration claims and identifying affected parties can contribute to up to 40 percent of the direct costs of a data breach.[8] Appropriate data protection regimes that detect and quantify potential exfiltration at the boundary and endpoints can significantly reduce these costs.

[3] Moore, Susan (2020). "Gartner Predicts for the Future of Privacy," Gartner. https://www.gartner.com/smarterwithgartner/gartner-predictsfor-the-future-of-privacy-2020/

[4] Sweney, Mark (2019). "Marriott to be fined nearly £100m over GDPR breach," The Guardian. https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico

[5] BBC (2019). "British Airways faces record £183m fine for data breach." https://www.bbc.com/news/business-48905907

[6] Verizon (2020). "2020 Data Breach Investigations Report (DBIR)," Verizon Enterprise Solutions. https://enterprise.verizon.com/en-us/resources/reports/dbir/

[7] Check Point Software Technologies LTD (2020). "Ransomware Evolved: Double Extortion," Check Point Research. https://research.checkpoint.com/2020/ransomwareevolved-double-extortion/

[8] Chubb (2020). "Chubb Claims Costs," Chubb Cyber Index. https://chubbcyberindex.com/#/costsbreakdown

Data governance and strategy

Uncovering business insights by interpreting, correlating and analyzing myriad data sources through artificial intelligence (AI) and machine learning (ML) is highly valuable for an organization's bottom line and customer engagement, but it also presents data storage and management challenges. Effective data governance aligned with business strategies is essential to minimizing risks and harnessing the data's full potential.

The maturity level of an organization's data governance is considered a true indicator of how organizations view and manage their data today — a fundamental shift that the industry is undergoing. Data governance almost always has multiple components at play, including people, physiology, organizational goals, timing, conflicts and external factors. Aligning data governance with corporate governance, therefore, heightens the data governance profile at the board level.[9]

Additionally, addressing alignment with business outcomes, defining the value of technology programs and understanding high-level requirements leads to practical roadmaps, designs, architecture and more.[10]

Strategy alignment focuses on the business benefits that must be derived from capturing and analyzing data (**Figure 1**). Managing data as an asset with the same diligence as other assets includes considering any associated liabilities or costs, as well as establishing effective policies and processes throughout the data life cycle — from the early stages of data creation to how it will be stored, used, shared, archived and then permanently destroyed. Organizations can use a policy-based data life-cycle management (DLM) approach to effectively manage the flow of data from beginning to end.[11]

Figure 1. Strategy work area and data governance (DG) considerations

Policy and process

A data-centric approach to security is widely recognized as effective in protecting information assets throughout the life cycle. Typically, data protection policies are well-defined. But, determining how to implement the security strategy with controls that actually reduce risk is often less clear, and implementation challenges multiply when priorities and outcomes are defined by technological capabilities rather than the logical design of the organization's security processes. Such dysfunction typically presents as "aspirational security" — established data classification policies, but weak control standards and chronically suboptimal implementation

[9] Pearce, Guy (2017). "Align Data Governance with Board Governance Imperatives." The Data Administration Newsletter. https://tdan.com/align-data-governance-with-board-governance-imperatives/21355

[10] Ladley, John (2020). Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program. Second Edition.

[11] Rouse, Margaret (2010). "Data Life Cycle Management (DLM)," SearchStorage. https://searchstorage.techtarget.com/definition/data-life-cycle-management

A principled, top–down, outcome-led approach aligns to and supports business and security outcomes. A model process is one that (1) discovers information within the organization; (2) applies an organization-approved classification process to protect such information assets; (3) secures information by applying appropriate protective controls; (4) monitors the confidentiality, integrity and availability of information assets; (5) responds to alerts relating to changes in protective and detective controls;. (6) automates corrective actions to ensure ongoing security of the information assets; and (7) verifies the status of assets and their controls throughout their life cycle. These steps form DXC Technology's Data Protection Reference Process, outlined in **Figure 2**.

Figure 2. DXC Data Protection Reference Process

Once control objectives are set, a vendor-selection process can review the available market capabilities and design a solution that addresses the gaps of any one particular control system. The solution needs to conform to established enterprise architecture standards and to appropriately specify, implement and respond to logs and events.

The written policy should be an achievable goal, not an academic exercise creating a document that no one will read or that merely sets a low enough bar to get board sign-off. A sound policy considers the organization's ongoing business transformation efforts and the implications for where (in the cloud, at the edge, on-premises, with suppliers) and how (privacy and consent) data will be used throughout its life cycle (creation, process, analysis, storage, access, archival and deletion).

Roadmap

Data protection covers a broad set of controls — constantly being refined and added to — for securing data throughout the life cycle.

In the short term, organizations can improve data governance of cloud workloads through cloud-based hardware security modules (HSMs) that let users import the keys they choose. A multicloud delivery model enables delivery-agnostic data protection policies and processes even though the HSM is no longer on-premises.

Cloud service providers (CSPs) have made strides in integrating machine learning into their platforms to automatically detect and classify data so that it is commensurately tied to appetite and budget, such as storing lower classification assets at a lower cost.

Information rights management (IRM) is also seeing wider use. Its popularity — compared to the slow and limited mass adoption of traditional Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) encryption — is largely attributed to Microsoft's inclusion of Azure Rights Management services in its E3 licensing, which allows employees to easily use secure email capabilities.

In the medium term, pseudonymization can be an effective control for meeting stringent regulatory (GDPR, CCPA, etc.) or other privacy requirements. Rather than transmitting copies of data between two entities, the sender and receiver agree on a common substitution algorithm to enter into and retrieve from an out-of-band system, and then transmit only a token between them. This mechanism can be useful to protect the privacy of the information, yet allow the receiver to perform business-critical tasks.

Industry alignment and best practices

In today's complex IT environments, businesses cannot afford to continue with siloed approaches to data security. Organizations must adapt their data protection strategies to span their entire data infrastructure and support all data types.

Most practitioners and security evangelists today agree that the right combination of detective and preventive controls makes overall security postures much stronger and would prevent many traditional attacks.

Securing sensitive data and combating today's threat landscape, while staying compliant with various ever-changing regulations, is not a trivial task. However, a data strategy can leverage effective processes, resources and tools to support a company's risk appetite and security requirements. When resources and budgets are limited and markets are increasingly challenging, prioritizing and using these resources effectively is crucial.

Use compliance as an opportunity to protect data

Achieving compliance with various local and state laws and regulations should only be a starting point, not the ultimate goal. An effective data security and protection system — including all the controls adopted to put it in place and continuously enforce it — serves specific business needs, not just compliance requirements. General security standards provide excellent guidance, but implementations must be based on factors unique to each organization, including:

- Risk assessments that relate directly to the business value
- Vulnerability assessments that consider exposures across the entire infrastructure
- Security controls, with the number of preventive and detective controls matching the outlined risk and business values

Various studies and surveys conducted by government and academic institutions conclude that a sizable percentage of data breaches are perpetrated using trivial and well-known web-based attacks,[12] stolen credentials, or by insiders with legitimately authorized access to the system and data. Securing data requires a proven and true defense-in-depth approach involving both technical and administrative functions that span preventive, detective and administrative controls.

The traditional paradigm of "trust, but verify" is being completely rethought and replaced by the more modern, bold, but robust and efficient Zero Trust approach of "never trust, always verify."[13] This motto applies not only to privileged users who have direct access to the host and database, but also to applications, workloads and serverless functions that might access the same database.

[12] Open Web Application Security Project. "OWASP Top Ten." https://owasp.org/www-project-top-ten

[13] DXC Technology. "Zero Trust for maximum security." https://www.dxc.technology/security/insights/148676-zero_trust_for_maximum_security

Most practitioners and security evangelists today agree that the right combination of detective and preventive controls makes overall security postures much stronger and would prevent many traditional attacks. In a SQL injection attack on a database, for example, the system would detect a privileged account being enabled and send a security alert in real time to an administrator during the attack.

Ultimately, organizations need to think holistically about the risk and value of the data they seek to secure.[14] Rather than stopping at compliance, they should view it as an opportunity to innovate and raise their security standards in a way that fully supports the business.

Adopt platform-agnostic security solutions

Organizations need to understand where their assets and data are located. More importantly, overarching security programs must build in mechanisms (such as policies and preventive controls) that are tightly coupled with business objectives and goals.

Data protection needs to dovetail with broader security efforts, particularly in heterogeneous IT environments that constantly change, grow and introduce new types of data sources, with sensitive data dispersed throughout. Organizations need to understand where their assets and data are located. More importantly, overarching security programs must build in mechanisms (such as policies and preventive controls) that are tightly coupled with business objectives and goals. Vendor-independent and platform-agnostic security solutions tend to bring about longer-term benefits in terms of sound technology investment than a given technology or solution.

An organization may be ready to take the next step and acquire a dedicated data security solution and skills when it:

- Recognizes the high value of personally identifiable information (PII) and other personal data, company-sensitive data and proprietary data, along with data that has regulatory implications (any combination of PII, IP, credit card numbers or other financial data) or that leads to other serious implications when lost or stolen.
- Finds that tracking and securing all its assets and networks (including cloud instances) are rapidly becoming daunting tasks — particularly true in dynamic and faster-growing organizations.
- No longer has a clear view of how its assets and resources are being used, so there is no way to understand exactly what is being spent and what is appropriate to spend across all its security activities, and therefore no way to accurately measure the return on security investment in terms of risk reduction.

A dedicated, platform-agnostic solution that integrates with the existing security team can range from advisors or consultants to more formal, contractual SLAs. Managed services, for example, can deliver a continuous, scalable and cost-effective solution that brings expertise and proven approaches to governing data.

Clearly define data owners

Data is typically spread and shared across business units. It often resides in hybrid cloud infrastructures that are governed by third-party SLAs and accessed by employees from mobile devices. More recently, internet of things (IoT) devices operating in potentially hostile environments and constantly sensing the world around us may also have ready access to this corporate data.

[14] TechTarget. "Holistic security." https://whatis.techtarget.com/definition/holistic-security

To effectively account for this data sprawl, organizations need a chief data officer (CDO) or data protection officer (DPO) who is dedicated to the well-being and security of sensitive and critical data assets. In fact, companies based in Europe or doing business with EU data now face GDPR regulations that require them to have a DPO.[15]

This requirement sets a positive example because it clearly underscores that sensitive data has value extending beyond the line of business that holds it, and that someone must be officially responsible for all data assets.

When outlining the objectives and responsibilities for this role, organizations should consider following standard best practices. Ultimately, a CDO or DPO should take the lead in developing data security collaboration between teams and across the enterprise.

To effectively secure corporate data, everyone needs to work together. Work groups and teams need to be open to collaborating under the guidance of the CDO or DPO, who should be dedicated to all the programs and protections an organization needs to secure its sensitive data.

Industry research shows that 5.5 percent of published vulnerabilities are being exploited in the wild.

Deal with vulnerabilities and ongoing threats

Industry research shows that 5.5 percent of published vulnerabilities are being exploited in the wild. In addition, many recent high-profile breaches have resulted from known vulnerabilities that went unpatched even after patches were released.

Given that attackers focus on a few vulnerabilities in the real world, a promising approach toward remediation is to identify vulnerabilities that are likely to be exploited, and therefore prioritize organizations' efforts toward remediating those vulnerabilities first. Failure to quickly patch known vulnerabilities puts an organization's data at risk. To meet these challenges, organizations must have an effective vulnerability management program — and the technology to support it.

Clearly, organizations need an effective vulnerability-management program — and the technology to support it. The right set of data encryption techniques and capabilities can help secure data against new and emerging threats. However, when designing a cryptosystem, it is important to fully consider its effective lifetime, because with sufficient time and computing power, all encryption can be broken. Ciphers and keys need to be properly generated, handled, rotated and updated by people with a deep awareness of the ever-changing threat landscape.

Very-high-risk and high-sensitivity data stores — PII repositories, company financial ledgers and intellectual property — call for the most robust encryption standards. However, companies can implement less robust techniques such as data masking for customers' legal names, birthdates, residential addresses and other publicly available data.

Proven tactical approaches also include low-cost, conventional deception technologies that generate traps and decoys, including DNS sinkholes and fake databases and servers. The methodology can prevent data discoveries and protect less-sensitive data such as auxiliary services, process-related ticketing systems and logging databases.

[15] Proton Technologies AG. "Complete guide to GDPR compliance," GDPR.EU. https://gdpr.eu/

Adopt data access management: Real-time monitoring for privileged access

Applying the Kipling method[16] — who, what, when, where, why and how? — when evaluating access to data is especially helpful for privileged accounts that are the most common culprits in insider threats. A data protection plan should include realtime monitoring of privileged users in case there is a malicious employee or someone whose credentials have been compromised.

To prevent possible malicious activity, a solution needs to identify outliers, block activity, conduct dynamic masking (ensuring that sensitive data is not shared) and quarantine user accounts associated with high-risk access activities.

Another way to govern access to sensitive data throughout its life cycle is by applying sensitivity labels — encryption, access restrictions, visual markings and more — linked to protection actions.

As companies rapidly expand and migrate their infrastructures, workloads and applications into the cloud, their data moves there too — along with the naturally higher risk associated with cloud databases.

Implement automated detection and protection as a strategy

When starting on a data security journey, organizations need to size and scope monitoring efforts to address business requirements and risks. This often involves adopting a phased approach to developing and scaling best practices across the enterprise. Ideally, organizations should begin by prioritizing a subset of the most sensitive data, making sure data security policies are clear, tight and successful before extending them to the rest of the infrastructure.

At the very least, organizations should deploy automated systems to monitor data at the file level, or better, at the transactional level. Analytics in these systems can identify unusual behavior and risks to key assets and trigger automated data protective controls that are optimized for the business.

Many organizations start by implementing automatic, built-in security alerts that detect abnormal behavior by monitoring data, transactions or file activity. Usually, only more sophisticated and mature data security deployments leverage capabilities such as dynamic data masking or blocking. These include policies that, for example, reveal only the last four digits on credit cards to customer service representatives, while showing the full credit card number to customer service supervisors.

As organizations develop data activity monitoring and protection plans, they should continuously assess the evolving business risks to the assets and data and then align strategies accordingly.

Employ 'smart' (AI and ML) approaches to protecting data on-premises and in the cloud

As companies rapidly expand and migrate their infrastructures, workloads and applications into the cloud, their data moves there too — along with the naturally higher risk associated with cloud databases. Cloud providers may be managed by various personnel, operating by their own policies and procedures that often are not controlled by the organization consuming these services. Adding to the complexity, many prominent sources and surveys show that the trend is to use multiple cloud providers.[17] When data is managed in more than one place under multiple arrangements, classifying and tracking it becomes even more critical.

[16] Changing Minds. "The Kipling method (5W1H)," Creating Minds. http://creatingminds.org/tools/kipling.htm

[17] Luxner, Tanner, "Cloud Computing Trends: 2021 State of the Cloud Report," Flexera. https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/

Machine learning helps to simplify complex data scenarios. It can identify sensitive data and leverage dashboards and alerting tools to increase visibility and insights into how it is being accessed or moved. "… ML is a fast-growing trend in security management and monitoring. Analysts at ABI Research estimate that machine learning in cybersecurity will boost spending in big data, artificial intelligence (AI) and analytics to $96 billion by 2021, while some of the world's technology giants are already taking a stand to better protect their own customers."[18]

Adopt policy-based, converged, cloud-delivered, secure access service edge

Organizations today are finding themselves amid a tectonic shift from traditional security approaches to new ways of working and storing, transporting and accessing data. At these fault lines, some approaches are falling away while new technologies are emerging.

As more users, devices, applications, services and data move outside a company's perimeters, the complexity of traffic communication multiplies.

For the modern digital business to be effective, scalable and dynamic, network security architects can no longer afford to base connectivity requirements on the enterprise data center. The future of network security is in the cloud, which is why Gartner recently introduced a new paradigm for software-defined secure access: Secure Access Service Edge (SASE). Gartner predicts that by 2024, at least 40 percent of enterprises will have explicit strategies to adopt SASE. Additionally, an increase in GDPR and other worldwide regulatory data privacy requirements will create enterprise demand for SASE policy-based traffic handling for inspection, routing and logging to a specific geographic jurisdiction.

As more users, devices, applications, services and data move outside a company's perimeters, the complexity of traffic communication multiplies. The clear need to decrypt and inspect encrypted traffic once it leaves an organization will increase the demand to consolidate networking and security-as-a-service capabilities into a clouddelivered SASE setup. Organizations will need to devise policies and controls focused on the context of data throughout its life cycle and movements, and incorporate these policies into SASE tools that secure the perimeter-less enterprise environment.

Even traditional on-premises data center monitoring technologies such as data loss prevention and secure web gateways are now essential components of this new dynamic, highly scalable, cost-effective, software-defined architectural paradigm.

[18] Allied Business Intelligence, Inc. "AI & Machine Learning Research Service," ABI Research. https://www.abiresearch.com/market-research/service/ai-machine-learning/

Conclusion: Building an effective data protection and governance regime

Data has become the lifeblood of corporations. Because its collection and use are today's revenue streams, data is increasingly coming under scrutiny. With higher exposure, organizations need to clarify their data security position and understand what is expected of their electronic data assets — or risk consequential losses to reputation, brand and the ability to trade.

As business models and data protection practices have been evolving to take advantage of new technologies and markets, social norms have also been shifting. Data commoditization has led to privacy concerns and global adoption of more data protection and privacy laws. The impact of what may have been considered an acceptable business practice a year ago may now be more fully understood and considered unacceptable.

Analogous to Lawrence Lessig's pathetic dot socioeconomic theory (where law, social norms, the market and architecture constrain our actions), the interplay of technological progress and societal norms defines the parameters of an enterprise's data protection strategy.[19] These two forces naturally inform an organization's risk posture, which in turn binds the strategy of how and what data the organization manages. Without proactive and thoughtful management of the data life cycle, companies may experience increased liabilities or expenses.

An effective data protection and governance regime, strategically aligned to an organization's objectives, will help to reduce risks and enable business innovation and success.

[19] Lessig, Lawrence (1999). Code: And Other Laws of Cyberspace. Basic Books. ISBN: 0-465-03912-X

About the authors

Simon Arnell, security chief technologist, United Kingdom and Ireland, for the Office of the CTO at DXC Technology, has a background in applied security research and development and in running customer proofs of concept. Previously Simon led the commercialization of the DXC DNS monitoring service and pioneered the use of software-defined networks for rapid incident response, as well as the application of stochastic process modeling and simulation for strategic security-policy decision support. Simon's body of work is supported by several awarded patents.

Bex (Hirdman) Nitert, managing consultant, Cyber Security and Forensics, ParaFlare, undertakes digital forensic investigations following suspected security incidents and assists customers with identifying the nature and scope of information exposed in data breaches to support compliance activities. Bex also leverages her insights from digital forensic investigations to identify control gaps and provide cybersecurity recommendations on consulting engagements. Bex previously worked for DXC Technology and also served as digital forensic lead in Australia for a global professional services firm, where she worked with law enforcement agencies, regulatory bodies, legal teams and corporations.

Firas Jan, Australia and New Zealand regional lead, DXC Technology Managed Security Services, focuses on digital security and the public sector in Australia. He has more than 22 years of IT experience working with government and various industries in information security, incident response, vulnerability and risk management.

Alex Kreychman supports one of DXC Technology's global aerospace and technology accounts as a cybersecurity engineer and also serves as the architect in areas of security service delivery, cyberincident monitoring/response, network edge/endpoint protection and encryption. Before joining DXC, Alex had over 18 years' experience providing technical and leadership expertise to protect various businesses in many security domains, including cyber risk management, security operations, cybersecurity architecture and compliance.

Learn more at
dxc.com/security

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.