GOVERNANCE

ACHIEVING DATA SECURITY AND COMPLIANCE

How to Safeguard Identity, Protect Information, Reduce Risk and Create Value

Microsoft

ISACA

CONTENTS

ABSTRACT

Over the last 20 years, the relative costs of computing power and data storage have plummeted. In that same time period, new technologies have evolved to provide enterprises with the ability to manage, maintain and process data anywhere and from everywhere.

Cost and complexity are no longer limiting factors in our digital universe, which has led to an explosion of data of every type—structured, unstructured, privileged, confidential and mundane. In order for businesses to be successful today, they need to consider the ever-increasing demands for real-time sharing and collaboration, which creates even more risk for the enterprise. Grappling with this growth of information is not just a challenge from a security standpoint, but also from ever-expanding regulatory demands by nation states and governments around the world demanding improved consumer and citizen privacy.

This white paper focuses on the evolution of data security and compliance, and the methods, processes and approaches you can take to unify the often competing demands of meeting regulatory obligations, while also achieving the information protection and user security that your enterprise must deliver to safeguard everything from intellectual property to corporate reputation. Methods for achieving compliance and security without compromising, but possibly enhancing, user productivity are also highlighted.

Introduction

Regulatory and compliance demands for data protection show no signs of slowing down in the foreseeable future. Technologies, such as application programming interfaces (APIs), are not only enabling the near frictionless flow of data between people, parties and applications, but are being used to build the foundation of frameworks, such as the Payment Service Directive (PSD2) and open banking[1] in Europe, the United Kingdom and Australia. The rise of cloud computing technologies along with APIs complicates the struggle for enterprises as they fight to achieve compliance and deliver security while managing legacy debt in the form of technology and process. For small mobile application providers to massive complex enterprises, the continued pressure and desire to monetize data is at odds with the need and obligation to protect and secure the same data. As enterprise digital transformation programs mature, the ability to transform and share data quickly becomes critical to business success. Easy access to even more data creates a perpetual loop for enterprises that are trying to secure information while facilitating the types of frictionless access that users want and need.

While enterprises move quickly to evaluate the actions that they need to take to stay compliant across all of their regulatory obligations, the fundamental truth that being compliant does not equal being secure is increasing the pressure on chief information security officers (CISOs), chief data officers (CDOs), chief privacy officers (CPOs) and other enterprise leaders to deliver security *and* compliance.

Information security domains that once were viewed as independent functions and only tied together in approaches, such as defense-in-depth using overlapping controls, are now being tightly coupled. Identity has shifted from purely an administrative management function to being accepted as the core of a secure environment. As data protection requirements become more onerous and challenging, one common theme has emerged that suggests a pathway to achieve both security and compliance. Data privacy regulations generally agree that the data requiring protection belong to an individual. The California Consumer Privacy Act (CCPA) states, "California consumers should be able to exercise control over their personal information."[2] The Global Data Protection Regulation (GDPR) of the European Union connects users to their data in several ways, including portability: "The data subject shall have the right to receive the personal data concerning him or her…in a structured, commonly used and machine-readable format."[3] By creating a direct link between a user, consumer or citizen and their data, identity security now becomes the steel thread required to achieve compliance success. While legal or regulatory requirements may be a driver for change, most, if not all businesses, have to address the information protection realities of their day-to-day operations to include intellectual property threat and insider-facilitated data exfiltration. Creating that direct link between a user's identity and their data, then, can yield benefits well beyond achieving compliance.

[1] Manthorpe, Rowland; "What Is Open Banking and PSD2? WIRED Explains," *WIRED*, 17 April 2018, www.wired.co.uk/article/open-banking-cma-psd2-explained

[2] California Legislative Information, "AB-375 Privacy: personal information: businesses (2017-2018), Section 2(h)," 29 June 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[3] GDPR.EU, "General Data Protection Regulation (GDPR)," https://gdpr.eu/article-20-right-to-data-portability/

Buried in Data

In this era of easy data, easy development and easy access to data, the ability to deliver solutions at high velocity has resulted in eroding, not improving, data security and privacy management. At the advent of the modern digital age, data control was as simple as system access control. Air gaps, a common reference to systems or sources not on the network, were not by design; they were simply operational realities.[4] Data control was achieved because the preciousness of computing power and storage necessitated limited and responsible use. In a world defined by ever faster personal device processing and always accessible data, the control and security of the data has diminished at the same inverse rate. Some studies suggest that data are growing at a compound annual growth rate of 61 percent,[5] while security breaches over the last five years have increased by 67 percent.[6] As data growth has accelerated, the direct correlation to increased security incidents is clear.

Beyond the increased risk of exploit and breach, the fundamental problem with data growth is that it is not delivering a corresponding return in value. The exploding volume of data is not running 60-percent more processes, but, instead, is redundant, unclassified, often unnecessary and frequently unmonitored. Only with the rise of recent regulatory and compliance demands has the challenge of wrapping security and protection around all of this data come clearly into focus. Regulations clearly demand that enterprises have a full grasp and complete classification of data, regardless of where their data reside.

Regulations clearly demand that enterprises have a full grasp and complete classification of data, regardless of where their data reside.

Acknowledging that there is a data problem in on-premise and cloud-born systems, data stores and end-point devices is the first step to building an effective data security and compliance program. Regulations do not differentiate between data in a system of record or data in a spreadsheet that was created three years ago by a marketing intern. It is not enough to meet today's compliance requirements; enterprises must also build a program that anticipates and keeps pace with the future.

What Is Changing?

Enterprises are starting to realize that an organizational separation between information security controls and data privacy requirements delivers suboptimal results in the effort to achieve compliance and security. This independent development of the privacy and security functions has resulted in a disjointed approach that leaves data at risk.

Although this separation has been the status quo for decades in the enterprise, a shift is underway.[7] This shift

[4] Zetter, Kim; "Hacker Lexicon: What Is an Air Gap?" *WIRED*, 8 December 2014, https://www.wired.com/2014/12/hacker-lexicon-air-gap/

[5] Grey, Victoria; "Data Growth Statistics to Blow Your Mind (or, What is a Yottabyte Anyway?)," APARAVI, https://www.aparavi.com/data-growth-statistics-blow-your-mind/

[6] Bissell, Kelly; Ryan M. LaSalle; Paolo Dal Cin; "Ninth Annual Cost of Cybercrime Study," *Accenture,* 6 March 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[7] US National Institute of Standards and Technology (NIST); *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0*, 16 January 2020, www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

will drive enterprises faster than any regulatory or compliance demand possibly could. Recently, Equifax announced that it had combined its data security and data risk efforts into a unified program,[8] using US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and an Equifax® privacy framework, and capitalizing on the resultant risk reduction achieved by joining identify, protect, detect, respond and recover controls. The new NIST Privacy Framework tightly couples privacy to key NIST CSF functions.[9]

Enterprises are looking for a different way to achieve security and compliance. No privacy regulation to date has played a tangible role in stemming the rapidly increasing number of breaches or the exfiltration of data that enterprises are experiencing today. Some large enterprises are leading the way in the development of a new best practice—combining data security with data privacy, leveraging identity.

It Does Not Get Easier From Here, So What Do I Do?

Managing privacy and security will not get easier. Nation states and local governments are showing no interest in either holding protections and demands static or reducing their amount and degree of oversight. Unfortunately, bad actors are not paying attention to any regulations either, as cybercrime losses continue to increase year over year.

Many industry and trade groups are working with legislatures around the world to craft regulations that couple security and privacy, e.g., the Apple® announcement of its single sign-on (SSO) service in 2019 and the continued expansion of the Microsoft® integrated security capabilities across its suite of products.[10] The escalating costs of fines, legal expenses and recovery are in the hundreds of millions of dollars[11] for single-breach events at large enterprises. The question is not if the enterprise will do something to bring data security and data privacy together, but when. When is now.

To create a secure data environment that improves compliance performance while empowering individuals in the enterprise to be active parts of the solution is by capitalizing on the connection between identity and data.

First, Make the Connection

The tight coupling of a user's data to the user's identity safeguards data and effectively secures the enterprise from attack and breach through phishing, malware, ransomware and other methods that have dependencies on effective social engineering. The use of social engineering is growing at a pace in excess of 17 percent per year[12] and is clearly the pathway of choice for bad actors.[13] This information suggests that enterprises not only need to join data and the user, but also empower users as Microsoft does through its security and compliance capabilities integrated with, for example, Microsoft Office applications.

[8] Wright, Lydia; "Equifax Comments to Draft Framework," 24 October 2019, www.nist.gov/system/files/documents/2019/10/29/l_wright_equifax_official_comments_to_draft_nist_pf_20190225_508.pdf

[9] *Op cit* NIST, page 17, Appendix A

[10] For more information, see www.microsoft.com/security.

[11] Shen, Lucinda; "Capital One's Data Breach Could Cost the Company up to $500 Million", *Fortune,* 31 July 2019, https://fortune.com/2019/07/31/capital-one-data-breach-2019-paige-thompson-settlement/

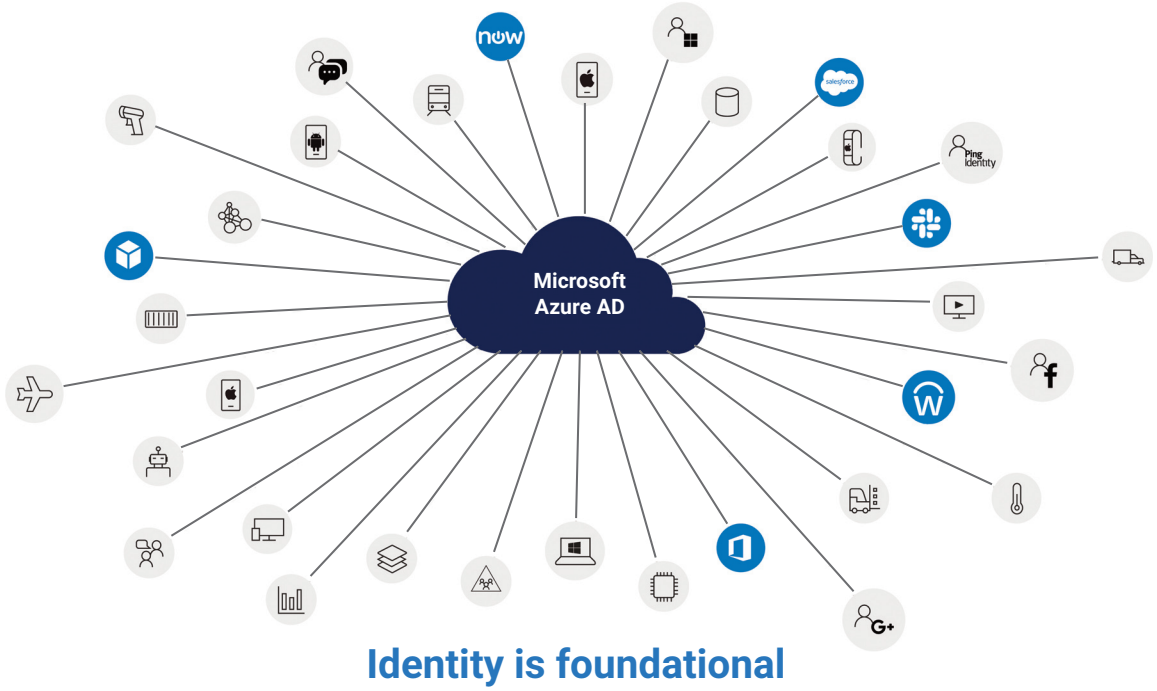
[12] FireEye, "New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks," 25 June 2019, https://investors.fireeye.com/news-releases/news-release-details/new-fireeye-email-threat-report-reveals-increase-social

[13] Proofpoint, "Global State of the Phish Report Finds Social Engineering Cyberattacks and Credential Compromise Jumped in 2018, 24 January 2019, https://www.proofpoint.com/us/newsroom/press-releases/global-state-phish-report-finds-social-engineering-cyberattacks-and

A complication that most enterprises face in meeting their compliance requirements is that legislators and regulators globally have not always been mindful of the technical feasibility of the mandates they create. Although regulators have pursued citizens' right to be forgotten, regulators have displayed little understanding of the technical difficulty in that endeavor and, in many cases, have exempted entire functions, such as government services, from the technical demand while holding corporations accountable for performance. The lack of technical understanding is also displayed in the creation of regulations that do not acknowledge the interconnectedness of data, systems and users. For example, research, such as in the Verizon "Data Breach Investigations Report,"[14] shows that identity and misused credentials are the pathway to data theft. However, most regulations only suggest "reasonable security" while providing no guidance on what frameworks or standards are considered acceptable. With no explicit requirements defined, companies are left searching for best practices or making internal judgment calls on what meets the reasonableness test.[15]

Data privacy, in isolation, provides no meaningful risk mitigation to enterprises that are seeking to be both secure and compliant. Identity control is foundational to data security and privacy (**figure 1**).

FIGURE 1: Identity is Foundational



Source: Microsoft® Corporation

Although the needs and demands related to protecting identities in highly regulated banks are different from those in technology enterprises, such as Facebook and Google, identity is critically important to all enterprises,

[14] Verizon, "2019 Data Breach Investigations Report," https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[15] *Op cit* California Legislative Information

whether under the mandate of a regulatory requirement for employee access or a demand for trust by consumers. In 2019, Citibank declared that banks were the rightful creators and holders of unique, federated digital IDs.[16] Not by coincidence, just a few weeks prior, Facebook's Libra white paper states, "An additional goal of the association is to develop and promote an open identity standard. We believe that decentralized and portable digital identity is a prerequisite to financial inclusion and competition."[17]

Nation states and enterprises in every industry are creating unique digital identities for users specifically for the purpose of creating a tight join between a human and their data. Enterprises are beginning to realize that identity has been the area of least focus and investment among critical security controls for decades.[18]

Who Can Help?

Comprehensive solutions to secure data while being compliant are relatively limited. The rise of cloud-based infrastructure as a service (IaaS) and software as a service (SaaS) has not delivered on the promise of replacing on-premise infrastructure and business-critical application management. Enterprises have not completely replaced their data centers with the cloud; the cloud has become an additional deployment strategy for enterprises to manage on top of their other investments.

For myriad reasons, including resilience, optionality and maturity, many enterprises are settling on both a hybrid and multi-cloud strategy. This is the inevitable landscape for the foreseeable future.

To best understand how to create a combined data security and privacy program, enterprises need to look to solution providers that reflect this diversity and to find solutions that can help address compliance requirements while minimizing the effort the enterprise needs to expend in these efforts. For example, Microsoft provides a useful set of platforms, tools and capabilities.[19] Microsoft also embraced the value of the cloud, mitigating concerns about availability, up-time and redundancy, while helping users meet compliance requirements.

Put Identity in the Middle

For decades, security architectures have placed data or digital assets at the core of their diagrams and maps. Identity has been pushed to the outer tiers of these architectures, enforcing the notion of protecting things before protecting people. Probing the security architecture diagrams used by large and medium-sized enterprises reveals an asset in the center of the diagram that is surrounded by layers of controls and technologies. Zero trust has helped pave the way to identity-centric security thinking and innovation because of one of its key premises: "A way to think about cyberthreats is to assume you have already been compromised; you simply don't know it yet."[20] Assuming a breach means that it is not enough to know where data are and how they are

[16] Citigroup Inc., "The Age Of Consent: The Case for Federated Bank ID," 2019, https://www.citi.com/tts/sa/flippingbook/2019/the-age-of-consent/gra30727_TTS_age_of_consent/

[17] Libra, "The Official Libra Whitepaper, Section 05 The Libra Association," 2019, https://libra.org/en-US/white-paper/

[18] Gartner, "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," 15 August 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[19] For more information, see www.microsoft.com/en-us/security/business/information-protection.

[20] Forrester, "Zero Trust," 2020, https://go.forrester.com/government-solutions/zero-trust/

protected, but enterprises must know the identities and actors accessing and using the data internally and externally, without fail.

Assuming a breach means that it is not enough to know where data are and how they are protected, but enterprises must know the identities and actors accessing and using the data internally and externally, without fail.

Embracing an identity-centric approach to security and compliance requires a necessary expectation that humans play the critical role in the success of the program. An identity-centric security framework acknowledges the fundamental importance of the human element for the entire enterprise.

The issue with security frameworks and regulatory schemes is that neither places the person in the center of security or compliance. Data privacy regulations clearly place data at a higher level of importance than the actual user or owner of the data. No data privacy regulations have a mandate or demand for securing and protecting the user. Instead, these schemes call for protecting data and barely reference any forms or methods of security.

Understanding the human element is the first step in changing the results and outcomes within an enterprise. The diversification of infrastructure and application deployment choices has made this beginning exercise more challenging than it was several years ago. Enterprises need to uncover not just its users, but the different personas they exhibit as humans leveraging a host of available assets and systems that are inside the walls of their enterprise data centers, hosted by solution providers or that are running in cloud environments and instances around the globe.

A benefit of using Microsoft as a model for this discussion is that the ubiquity of Active Directory® (AD) and Active Directory Federation Services (ADFS) provides an identity source that has an association with everyone in an enterprise. In enterprises that have capitalized on the native capabilities of Windows Server® 2019 and Azure®, the ability to understand the entire population of users and their respective rights, privileges and entitlements is even greater.

It is critical, when identifying the user population, to understand the quality and the risk of identity-related data. Good identity directory hygiene is a must for all data security and data privacy efforts. In the course of putting identity in the middle of security architecture, enterprises should give strong consideration to conducting hygiene on directory systems. A best practice to consider is exercising a zero-trust approach to the current veracity and accuracy of directory data.

Understanding the human element is the first step in changing the results and outcomes within an enterprise.

Enterprises that are seeing the biggest leaps in maturity in their data security and privacy programs have begun to coordinate the creation of security-focused directory templates through the collaboration and cooperation of their infrastructure, security, privacy and business application owners. Standing up a brand-new directory may seem like an aggressive approach, and it will be one that takes planning, courage and leadership. Beyond creating a security-oriented record, effort will need to be expended to migrate current users to the new directory and then have a command center to monitor accounts and records that have unknown origins, unlisted or nonexistent owners and mysterious purposes. The likelihood of embedded credentials impacting a production process or system is high, but using a command-center approach achieves two important outcomes for the program:

- Enterprises will uncover these embedded credentials and their purpose, and immediately reduce risk upon mitigating those accounts within its systems.
- A significant amount of risk will be reduced by correcting the practices of the past, whether they are the nesting of groups or allowing free-form text entry into fields that should be tightly controlled.

Recognizing few enterprises will have the luxury to build a new directory, some tactical measures enterprises can take to improve include:

- Taking a cloud-first approach even with identity and access management services. Extend existing directory infrastructure to the cloud to get both the digital transformation and zero trust journeys off the ground.
- Increasing the trust of the directory by leveraging threat intelligence and implement capabilities such as multi-factor authentication.
- Implementing ongoing hygiene initiatives to improve provisioning/de-provisioning processes.

However, taking the time necessary to build the program on a foundation of high-quality user data is an effort that will reward perpetually. Bypassing this recommendation will cause disappointment, frustration and elongated implementation cycles, and result in a solution suite and process catalog that will be neither secure nor compliant.

Process and Tools Next

An early challenge to the program will be that current-state processes, both business and technology, will be tightly aligned to the asset-based security perspective of protecting data first and people at some lower priority. An example of process changes that will need to be considered is data discovery. Most enterprise data discovery processes and policies are specifically focused on what type of data resides in which location or store.

Data discovery is rarely coupled to users and owners in a granular way. The owner is considered a less important characteristic than the data sensitivity itself.

The availability of solutions, like Microsoft Information Protection, created an environment where data that falls into dozens of predefined protected or sensitive categories can be sorted out, and that data can be understood and associated to the user. This is a critical differentiation, because, unlike typical data discovery efforts, the enterprise can understand the relationship between the user and their data. A corporate officer or a member of the legal team might have perfectly rational and defensible reasons for having access to confidential and privileged information. By changing the process lens to include a unique data owner, the enterprise can achieve levels of operational efficiency and user satisfaction that cannot be attained with the old processes of simply locking down sensitive data stores. By using Microsoft Information Protection, the formerly arduous effort needed to classify data can now also benefit and be accelerated through automation. Auto classification, in combination with the empowerment of users to be an active component in the data security efforts yields a new set of capabilities that will return rapid dividends in understanding what data needs to be safeguarded.

Data discovery capabilities also allow an enterprise to root out data in business-approved sources and in informal or unstructured locations. Data in spreadsheets or archived email inboxes or file shares have commonly been exempted from data discovery processes as organizations have either focused their attention on data sources that are deemed critical to business or technology processes or have been excluded because technology solutions were not able to effectively search these other data stores. Regulatory and compliance

demands for data privacy do not differentiate between confidential information that is housed in a system of record or data placed inside of a well-meaning employee's spreadsheet to keep track of participants in the office bowling or golf league.

Data leakage is frequently tied to unauthorized or unstructured sources. Regulators will not go softly on enterprises that have had data breached or exploited because they were in a spreadsheet instead of a monitored database. For example, the diverse capabilities within Office 365® used in combination with the device-level functions of Windows Information Protection, provide the ability to more effectively contain the most common sources of leakage. Incorporating access rights management and document-level control in a way that does not require extensive training of the user will also be useful to limiting data leakage. When the user population is understood and their data and identities tightly coupled, there is an opportunity for empowerment that will change the effectiveness of enterprise efforts to be both compliant and secure. Turning users into an active component of security efforts is finally an achievable goal.

If You See Something, Say Something

With the user population identified and data uncovered, deep classification is the next critical step on the journey. In the past, one of the roadblocks faced by data classification programs has been the inescapable pace of data growth inside of enterprises. Many enterprises have successfully created and implemented the type of data classification and data governance processes required to show cursory compliance with many privacy regulations. Even at their advanced level of data privacy maturity, many of these enterprises have struggled mightily with applying classification labels to new and old data.

In workplaces, communities and public spaces, people are frequently the difference in situations that could go wrong. Whether reporting a suspicious piece of baggage in an airport waiting area or calling in an emergency when something is clearly awry across the street, people can be the difference. Yet, in the digital world, the person has been relegated to a task on a checklist.

The engagement between privacy organizations and humans is even more tenuous. Policies and processes are established in vacuums based upon regulatory and compliance demands, and regional or local laws, without input from the most-valued assets.

People are naturally attuned to the notions of privacy and security, if from no other source than the basic need for self-preservation. Not only can the user be an effective force in security but, by providing a pathway to enable their participation, can also have an incredible impact on enterprise performance in security and compliance.

Incorporating the user into the process flow presents unique challenges. The features available within Microsoft Information Protection provide a model in action that achieves the goal of having users be a key part of the defensive strategy. By manifesting choices that are already the most likely classifications that a user may need to apply to a document, an email or a file running on the user's preferred device application, Microsoft has created an effective engagement model that brings the user into the data protection fight. There is an understandable criticism that could be made that users will simply take the path of least resistance and mark every document as "public" or "general." By coupling security awareness training with tools and techniques that

users can leverage to create highly secure documents, data and assets within the enterprise, the risk of data leakage and exfiltration can be reduced by Microsoft's ability to provide "under the hood" automated classification which also mitigates the potential for users to under-classify data.

Enterprises can connect the strengths of their data management, identity authentication and authorization abilities, and their privacy policies to arm every employee with the tools and integrated capabilities of Microsoft 365.

Inspect What You Expect

A critical and continuous component of security and compliance programs is a natural evolution of all the work exerted to reach this point. The enterprise now understands its data better than ever before, and it has created processes that do not just tactically solve the problem of that day but produce evergreen results which keep data safe and compliant. Users are empowered and enlisted to be a direct complement and component of security and privacy programs.

With the uplift in these capabilities and the strength of the technical underpinnings that are driving levels of automation, monitoring the program becomes significantly less burdensome. The broader coverage of data protection across a much larger and deeper volume of data, combined with a well-structured and understandable classification method, will result in a greater capability to leverage rules and alerts in a more precise manner. The reduction in alert fatigue and false-positive driven operating procedures (turning off problematic alerts, etc.) will drive risk reduction and allow security and privacy resources to focus on true issues and threats more effectively. A potential cascading benefit of this powerful combination of data governance and technological enablement is the reduction of duplicative or "hoarded" data, further reducing risk within an organization by shrinking the data-related attack surface.

A World of Opportunities

Creating a tight bond between a user and the data they own or control improves security and compliance in the moment. However, these controls should be combined with evolving technology trends and other identity and data controls. This combination ultimately contributes to a more secure and compliant organization that benefits from the risk reduction achieved.

The most pressing example of how improved data security and compliance efforts will yield additive value to risk and security posture is the rise of APIs as a means for identity and data control. Although APIs were originally developed to facilitate the connecting of independent or disparate systems or processes, they are now being used more frequently to create a strong tie between users and their accesses to systems, services and data. As APIs create opportunities for improvement and automation of functions, ranging from user authentication to authorizing data access based on roles, physical location, device address and a nearly endless supply of additional attributes, the benefits of the program should be clear and exciting. Enterprises that have moved to an identity-centered framework will realize even greater benefits from an environment that is functionally preconditioned to capitalize on API-driven security.

The program efforts to mine data from such a broad range of sources and apply classification tagging will also result in a much more detailed understanding of data that are redundant or unnecessary for operations. Coupling a data-reduction program to these capabilities will reduce additional risk, because deleted data no longer represents a desirable target or threat. Enterprises may see a reduction in expenses as they eliminate the costs associated with ballooning storage demands.

Summary

For years, the mantra of the CISO has been that compliance does not equal security and privacy cannot be achieved without security. Data privacy regulations also have sprouted up all over the world over the years. Meeting the compliance obligations demanded in Australia, the European Union, the UK, Hong Kong and the United States has forced enterprises to spend money and time checking the box. Unfortunately, the effort required to check those boxes does not return a corresponding value in terms of risk reduction for the enterprise. It is critical for enterprises to pioneer their own path of aligning or even combining their data security and data privacy programs to create an environment that is both secure and compliant.

Identity-centric security is the key to bringing this change to enterprises. Although regulations across the globe have not yet caught up to the reality that the tight coupling of data combined with expectations of protecting the identity of the owners of that data, this does not preclude enterprises from making that connection themselves. By taking this approach, the value-added capabilities of rich solution sets, like Microsoft 365 and Microsoft Information Protection, dovetail into a program that unifies data, security, privacy and user experience in a way that results in improved compliance and reduced risk. With this realization, the requirements for evaluation of data security, data privacy and risk reduction programs clearly come into focus. The program must embrace:

- Discovering the purpose, use and location of data inside and outside of the enterprise.
- Observe the environment with an identity-centric eye and identify users who own the data.
- Identifying the sensitivity and criticality of the data.
- Implementing solutions that buckle the data and user together and improve how the data are protected, while empowering the user to be a part of the solution.
- Enable continuous monitoring of the processes, solution and users to ensure that security and compliance is being achieved.
- Focusing on risk in a continuous and effective manner, and continuous learning about the security technologies and how to utilize them effectively.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Richard Bird
Chief Customer Information Officer, Ping Identity, USA

Expert Reviewers

Melissa DeCapua
DNP
Microsoft, USA

Adham Etoom
CRISC, FAIR, GCIH, PMP
Government of Jordan

Mohamed Aboul Farag
CISA, CRISC, CISM, CGEIT
Housing and Development Bank, Egypt

Mathew Holdt
CISA
Protiviti, USA

Meghana Jagdish
CISA, CISM
Illumina, USA

Monica Peña
CISA
PwC, Ecuador

Hemma Prafullchandra
Microsoft, USA

Goh Ser Yoong
CISA, CISM, CGEIT
Jewel Paymentech, Malaysia

Board of Directors

Brennan P. Baybeck, Chair
CISA, CRISC, CISM, CISSP
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rolf von Roessing, Vice-Chair
CISA, CISM, CGEIT, CISSP, FBCI
FORFA Consulting AG, Switzerland

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Health Care Service Corporation, USA

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
AppGate Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
introSight Ltd., Israel

Rob Clyde
ISACA Board Chair, 2018-2019
CISM
Board Director, Titus and Executive Chair, White Cloud Security, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
Group Chief Executive Officer, INTRALOT, Greece

Greg Grocholski
ISACA Board Chair, 2012-2013
CISA
Saudi Basic Industries Corporation, USA

David Samuelson
Chief Executive Officer, ISACA, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

About Microsoft

Microsoft® (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

DISCLAIMER

ISACA has designed and created *Achieving Data Security and Compliance: How to Safeguard Identity, Protect Information, Reduce Risk and Create Value* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/data-security-and-compliance-2020

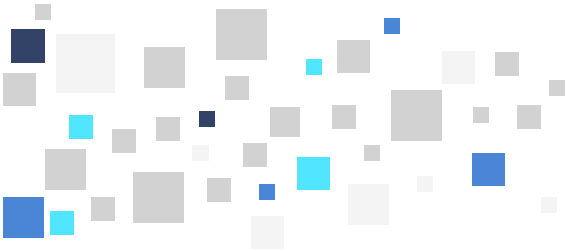
Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/



Data is exploding

Today, we create, store, and share data on all our devices, wherever work takes us. But, more data means more risk.

A balancing act

Protecting your data doesn't mean sacrificing productivity. By knowing where your data is, and how it is protected, you can collaborate confidently.

Privacy and productivity

Linking information protection, identity, and access management solutions enables users without hampering their productivity.

Know your data

An effective data security and compliance program leverages a four-stage lifecycle: discover, classify, protect, and monitor.

Solutions that work

Microsoft Information Protection is a built-in, intelligent, unified and extensible solution that can protect your data and keep you productive.

Microsoft

Learn more about Microsoft security and compliance solutions:

Information Protection website

Security and Compliance Adoption Guide

Information Protection blog

Information Protection white paper