The landscape from above: Continuous cloud monitoring for continuous assurance

Received (in revised form): 8th June, 2020

Fouad Khalil
Corporate Compliance Executive, USA

Fouad Khalil is a corporate compliance executive and is responsible for internal and external compliance programmes, auditor education, alignment with industry best practices, marketing support and sales enablement. With extensive experience in the technology space with more than 25 years spanning disciplines in software development, IT support, programme and project management and most recently IT security and compliance management, Khalil's career path in technology has provided him with keen insights in the areas of network, system and database administration, software programming, system software and GUI design, project and product development, solution implementation and much more. For nearly the past two decades, Khalil has focused on cyber security, data security, security investigations, security training and awareness, and security compliance, serving as an industry expert in key areas such as information technology (IT), National Institute of Standards and Technology (NIST), internal controls over financial reporting, Sarbanes-Oxley, PCI DSS, HIPAA, HITECH, GDPR and CCPA. Khalil holds a Bachelor's degree in electrical and computer engineering from Marquette University and CISA and ITIL Foundations certifications. Additionally, he is an active member/contributor in ISACA, IIA, Infragard, ISSA and ISC2.

Greater Boston Area, Massachusetts, USA
Tel +1-585-472-2356; E-mail: fkhalil65@gmail.com

Abstract The concept of monitoring information system security has long been recognised as sound and valuable management practice. For additional consideration, a large portion of compliance requirements for information security and privacy are supported by such monitoring. Security programmes must be aligned with privacy and compliance programmes to ensure those areas of data protection compliance are appropriately met and monitored, and then actions based on maturity levels must be aligned with information assurance programmes. Some key areas to consider in information security programmes include: 1) Continuous assurance (full data life cycle, continuous monitoring, continuous awareness, continuous compliance, challenges, benefits); 2) continuous supply chain management (continuous vendor management and oversight, benefits, challenges); 3) continuous cloud assurance (private cloud, community cloud, public cloud, hybrid cloud); and 4) continuous improvement (what is involved and necessary, including actions, monitoring and metrics).

KEYWORDS: continuous, compliance, cloud, technology, assurance, cyber security

INTRODUCTION

Moving from an on-premises to cloud-first or cloud-only IT strategy means adopting a wide variety of emerging technologies, many of which act as new threat vectors for cybercriminals. Artificial intelligence (AI), big data analytics, Internet of Things (IoT) devices and third-party cloud applications all connect to an organisation's critical infrastructure. While new technologies

streamline business processes, they also increase the potential for cyber and compliance risk. Problematically, many organisations understand the need to secure these technologies but find themselves overwhelmed by the sheer number of potential attack vectors. Whether service accounts or third-party services, the volume of cloud-based connections and monitoring locations becomes unmanageable as the organisation scales its digital transformation strategy.

Meanwhile, as organisations look to secure their ecosystems, they find themselves facing an onslaught of new regulatory requirements. Cyber security laws increasingly force companies to document their vendor risk management monitoring and oversight actions. Privacy regulations increasingly incorporate consumer litigation clauses. A single unpatched device or misconfigured cloud asset can lead to a data breach that compromises an organisation's financial and reputational stability. Traditional cost-benefit-risk analyses and point-in-time audits no longer protect companies when 'agile' applies to both corporate and criminal technologies.

To address the shifting risk landscape, organisations need to take a 'cloud's eye view' as part of their digital transformation strategies. They need to gain visibility over the new landscapes — both technology and compliance — to gain a full view of their cyber security risks. Continuous cloud monitoring that incorporates a combination of monitoring and risk alerts in conjunction with compliance aligned controls provides a way to reduce risks and establish a cost-effective continuous assurance programme.

MOVING FROM ON-PREMISES TO THE CLOUD: TECHNOLOGY ADOPTION IN THE DIGITAL AGE

Novel technologies began emerging in the late 1990s and early 2000s. The analyst firm Gartner estimates that by 2022, organisations will spend US$53.8bn on cloud business process services and US$151.1bn on software-as-a-service (SaaS).[1] Additionally, Gartner predicted that by 2020, 80 per cent of robotic processing automation (RPA) focused implementations will derive their value from complementary technologies.[2] In short, understanding the integrations between new technologies and security needs to be a priority for organisations attempting to secure their cloud deployments and mitigate compliance risk.

Cloud computing

Organisations contract cloud services to support business activities, making them part of the business environment but outside the direct control of the enterprise's IT department, so must be managed to mitigate information security and privacy risk, which varies across different kinds of cloud environments. A few findings from a recent report[3] highlight the challenges facing organisations while adequately addressing the new risk that cloud computing introduces:

- Sixty-five per cent of IT professionals still underestimate the damage cyberattacks against cloud-based targets can cause;
- Only 30 per cent of respondents affirmed security was the responsibility primarily of the cloud provider;
- Twenty per cent of organisations have experienced a cloud incident in the past year.

Without clearly documenting the security and privacy responsibilities governing the relationship, organisations find themselves struggling with ad hoc processes that can lead to compliance violations.

Big data analytics

Enterprises are increasingly migrating big data analytics to public clouds and creating more proprietary in-house applications food

supporting and integration analytics within the business environment. Since big data analytics produce three exabytes of data per day, companies migrate the processing to the cloud.[4] Whether using big data for customer service metrics, corporate financials or cyber security monitoring, organisations struggle to ensure that these sensitive assets are protected and that vendor public clouds meet necessary compliance requirements.

Bring your own device

Even before the coronavirus pandemic increased the world's remote work population, companies were struggling to manage personal device access to their networks, systems and software. Eighty-seven per cent of organisations allow employees to use personal devices to access business applications, perform processes or work with data files and 64 per cent of employees use personal devices for work, regardless of whether there is a policy in place or not; nevertheless only 59 per cent of organisations have a formal bring your own device (BYOD) policy in place.[5] With the rapid escalation of remote workers in 2020, employee device security and the risks associated with distributed workforces present an even larger obstacle.

IoT devices

IoT devices are becoming ubiquitous in business environments: 20.4bn IoT devices will be in use by 2020.[6] IoT devices and cloud services are inherently related, because most IoT devices are designed as end points that collect data for processing elsewhere, usually in cloud processing centres. IoT end points and cloud processing may mutually compound security risk and the complexity of assurance, because most IoT devices and apps are not sufficiently secure, if secured at all. In March 2019, US lawmakers introduced another bill to Congress hoping to establish regulatory security requirements.[7] As the security and privacy risks associated with IoT draw more legislative attention, organisations and their auditors need to create effective plans to manage them.

AI

New and emerging AI incorporated into big data analytics create business value by giving deeper insight into what the data means; however, along with these increased operational use cases come additional privacy and security challenges. Many information assurance professionals will need a plan to deal with these challenges effectively and cost efficiently since their budgets do not usually increase in light of risk associated with these new technologies.

From the top down: Security in the cloud

As companies migrate to the cloud, they need to restructure their cyber security approach. What works for on-premise security may not be effective in a cloud environment. Additionally, the regulatory requirements that place compliance and financial burdens on organisations seem to increase every day. Organisations need to start by securing their cloud infrastructure first, then bringing that security back to the ground. Unfortunately, the interconnected ecosystems, lack of clearly defined responsibility and pressures to scale rapidly increase rather than decrease costs and risks.

INCREASED PRIVACY RISK AWARENESS: THE LEGISLATIVE MANDATES

Data breaches not only increased in number and severity in 2019, but news outlets also took more notice of the breaches. A February 2020 ISC2 post noted that data breaches increased from 1,257 in 2018 to 1,473 in 2019 while exposed records decreased from 471,225,862 in 2018 to 164,683,455 in 2019.[8] Both personal and

corporate consumers increasingly took note of privacy while government legislation in the last few years exploded in response.

General Data Protection Regulation (GDPR) implementation

Implemented in May 2018, the GDPR put companies on notice that they must comply with privacy regulations or receive large fines. The GDPR gave privacy regulation teeth and elevated the focus on compliance by setting the compliance world into a tailspin. According to the website Privacy Affairs, 237 fines have been imposed for a total amount of €152,926,145.[9] The GDPR established the first extraterritorial law, applying the law to citizens living outside its borders or noncitizens living within its borders. This extraterritorial liability acts as the model for the regulations following the GDPR.

California Consumer Privacy Act (CCPA)

Similar to GDPR in extraterritorial jurisdiction, the CCPA applies to companies who sell to consumers living in or legally residents of the state of California. Building on the GDPR, the CCPA goes further by defining 12 data types, including biometrics, that organisations need to protect. The law inspired other state privacy laws, including those in Washington State, and federal legislative action, such as the US Data Privacy Legislation during the 116th Congress.

Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework

During the 2018–19 period, authorities began enforcing the SAMA Cyber Security Framework in an attempt to pressure other Middle Eastern countries to update their privacy regulations. SAMA appears to be meeting its goal. In June 2019, the Dubai International Financial Centre proposed additional Consultation Papers to better align the United Arab Emirates data privacy requirements with both the GDPR and SAMA.

New York Stop Hacks and Improve Electronic Data Security (NY SHIELD) Act

The 2019 NY SHIELD Act made a significant change in the way organisations review privacy. The law specifically shifted the definition of a data security event to incorporate both unauthorised acquisition of data and unauthorised access to data. This shift indicates an additional level of compliance controls necessary for meeting the requirements.

Australian Privacy Act

Further expansion of regulatory privacy requirements came from 1st January, 2019 update to the Australian Privacy Act which established a GDPR-esque extraterritorial extension to the law's reach, applying to owners/operators as Australian citizens/companies/subsidiaries. Similar conceptually to NY SHIELD, the Australian Privacy Act revision incorporated language focused on data 'at risk' which includes unauthorised access or disclosure that would lead a reasonable person to assume a likely harm. The law requires organisations to notify all 'at risk' parties, expanding the definition of affected parties beyond just users whose data was accessed or leaked.

National Institute of Standards and Technology (NIST) Privacy Framework

Most recently, NIST released its 'Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management'[10] in January 2020. The framework, although not legally binding, reinforced the importance of incorporating data processing ecosystem risk management as a separate risk from the traditional risk assessment.

A GLOBAL RESPONSE TO INDIVIDUALS' PRIVACY

Reviewing the last two years of regulatory and agency guidance updates provides valuable insight into the present and future of privacy compliance. Most legislative bodies and regulatory agencies appear to be coalescing on a shared set of best practices. Although the details differ between regions, organisations seeking to create holistic privacy compliance programmes can leverage the commonalities as they move operations to the cloud.

Everything is different, but everything stays the same

Despite geographic and regional diversity, many of the regulations contain similar requirements leading to a disjointed sense of overarching uniformity. Although suggested controls differ between regions, industries and companies, they all lay the groundwork of a similar foundation. The similarities indicate a global consensus of opinion regarding the value of personally identifiable information and corporate lack of appropriate protections.

Extraterritorial reach

Almost all of the post-GDPR legislation made a shift to incorporating 'extraterritorial' liability. For organisations to comply with these requirements, they must provide visibility into their market, the geographic location of their cloud services and the way in which they mitigate unauthorised access to these cloud storage locations. Additionally, organisations now must be more cognisant of the impact their digital global reach has on their compliance initiatives.

Definition of personal data

All the regulations and guidance in the past two years incorporated expanded definitions for personally identifiable data. For example, the GDPR defines a list of categories but also implies that the definitions should be interpreted broadly rather than being limited by the outlined definitions. Although the CCPA lists an exhaustively detailed 12 categories of data, it also includes inferences drawn from the categories that can be considered personal data.

Vendor risk monitoring

Privacy regulations follow the lead of their cyber security cousins, focusing on controlling how organisations share data and making them responsible for vendor controls. Data processors (GDPR), outsourcing (SAMA), collect/sell (CCPA) and data processing ecosystem (NIST) all refer to supply chain management. Despite the different terms, the underlying theme is the same. Organisations need to assess, mitigate and monitor vendor risk.

Board oversight

Seemingly taking their cues from other regulations like the Sarbanes-Oxley Act by increasing the board of directors' governance responsibilities. The GDPR applies personal liability while SAMA requires that the board approve funding, create an approving committee charter, and establish the governance, strategy and policy.

Civil lawsuits and fines

Although many of the regulations increased penalties for noncompliance, many of the regulations now allow citizens to bring private civil actions. Even more disturbing to many professionals is the addition of personal and professional liability they may incur from privacy violations.

The financial implications of the global response

Ultimately, all of these requirements increase the financial impact arising from

compliance activities and noncompliance. For example, according to the 2019 NetDilligence Cyber Claims Report,[11] during the five-year period that the report reviewed:

- Seventeen claims included regulatory defence;
- Ten claims included regulatory fines;
- Defence amounts ranged from US$2,000 to US$5.8m;
- Regulatory fine amounts ranged from US$5,000 to US$3.5m;
- Almost half of regulator fines claims resulted from a third-party data breach.

The increased number of regulatory compliance requirements when combined with the increased compliance fines and lawsuit costs mean that remaining a financially viable organisation relies on a strong privacy compliance posture. Understanding where an organisation's responsibilities lie and providing metrics that act as evidence proving governance, however, becomes more difficult as the organisation incorporates more emerging technologies and scales its digital transformation strategy.

CORPORATE RESPONSIBILITY: SHARING THE CLOUD SECURITY BURDEN

Cloud migration reduces an organisation's reliance on internal cloud computing resources, lowering costs and accelerating scale; however, with shared computing power comes shared responsibility. Meanwhile, companies moving to the cloud struggle to meet the shared responsibility model best practices. In October 2019, Gartner predicted that 90 per cent of the organisations that fail to control public cloud use will inappropriately share sensitive data through 2025.[12] Organisations looking to protect data privacy, however, face two significant struggles.

Controlling the cloud assets

RPAs, IoT, workloads and other cloud assets pose risks to cloud migration strategies. Rapidly spun and spun-down workloads can leave information in misconfigured storage locations. RPAs and IoT can be subject to credential theft. Each of these creates a new privacy risk that requires monitoring.

At a high level, the primary challenges organisation face was summed up in the ORACLE and KPMG Cloud Threat Report (2019)[13] report:

- Eighty-three per cent of cloud users have experienced security events due to confusion over shared responsibility security models;
- Ninety-three per cent of respondents are dealing with rogue cloud application usage;
- Only 1 in 10 organisations can analyse more than 75 per cent of their security events;
- Forty-five per cent plan to deploy automated patch management in the next 24 months starting with the database;
- Ninety per cent of chief information security officers (CISOs) are uncertain in their role in securing a SaaS environment.

From a compliance standpoint, companies lack clarity and visibility. They need to understand which cloud assets are their responsibility, but they also need visibility into the security of those assets. In terms of privacy compliance, both of these problems hinder effective risk management and governance.

Digging further into the technology issues, the McAfee Cloud Adoption and Risk Report (2019) highlights more detailed concerns facing visibility into cloud asset controls:[14]

- Average number of misconfigured IaaS/PaaS instance running at a time: 14;
- Average number of individual misconfiguration incident per month: 2,269;
- Number of AWS S3 buckets with 'world read' permissions: 5.5 per cent;

- Percentage of organisations with stolen cloud credential on Dark Web: 92 per cent.

As developers seek to meet project deadlines and follow agile processes, they often copy and paste code to deliver products on time. In other cases, they may not realise that they did not configure the assets individually. Each of these increases the organisation's cloud risk. At the same time, companies may be confused about who owns the risk and security responsibility.

Who owns what risk?

The first question organisations need to ask is whether they have an infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS) model. In multi-cloud ecosystems, they may even be deploying both models. In this case, then, the organisation first needs to define the type of cloud service they use and their own responsibility as part of that model (see Figure 1).

IaaS

Organisations using the IaaS model outsource the hardware, storage, servers and data centre space/network components, and possibly some software.

In this case, the cloud services provider is responsible for securing:

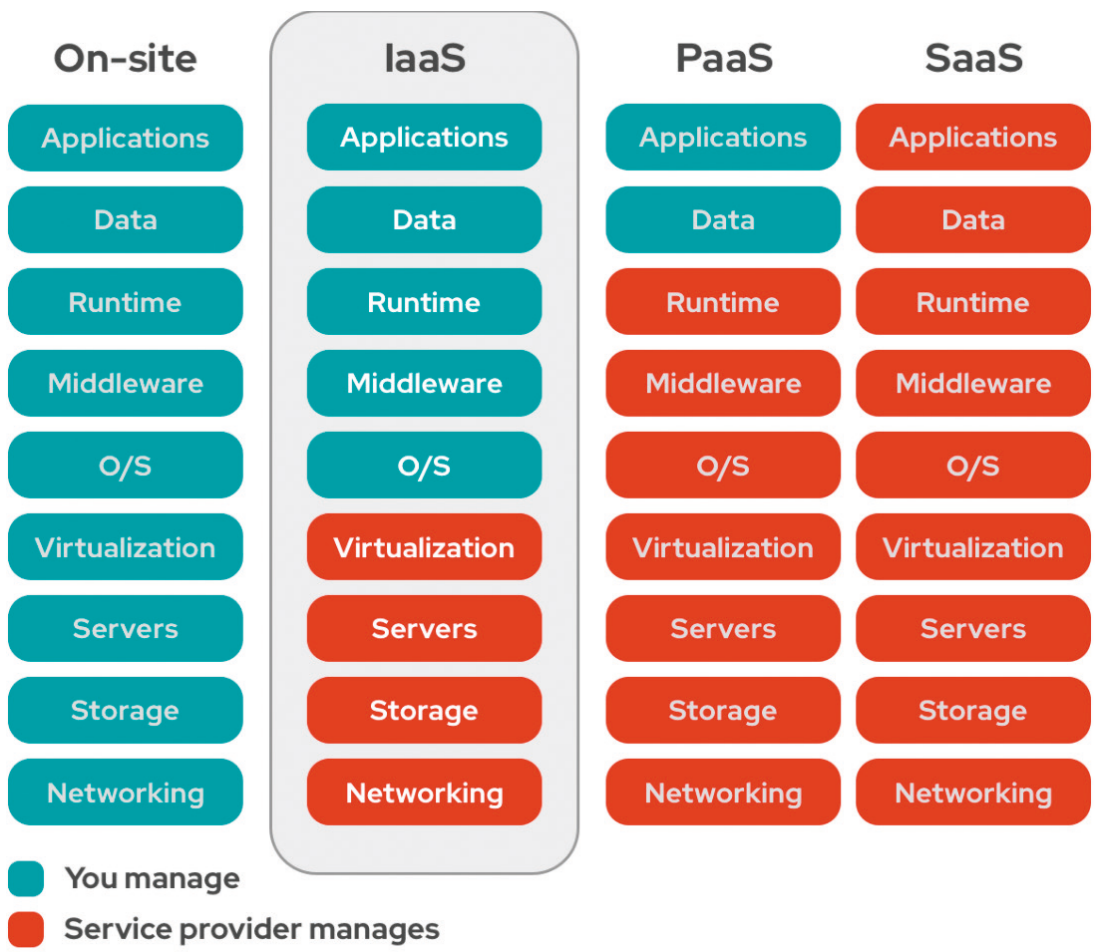

Figure 1: IaaS vs. PaaS vs. SaaS
Source: Red Hat

- Virtualisation;
- Servers;
- Storage;
- Networking.

Meanwhile, the organisation remains responsible for securing:

- Data;
- Applications;
- Middleware;
- Operating systems;
- Runtime.

PaaS

Under the PaaS model, the organisation leverages the cloud services provider's computing platform including operating systems, programming language execution environment, database and web servers. When organisations use a PaaS model, they outsource more services, which changes the risk and security responsibilities.

In this case, the cloud services provider is responsible for securing:

- Runtime;
- Middleware;
- Operating system;
- Virtualisation;
- Servers;
- Storage;
- Networking.

Meanwhile, the organisation remains responsible for securing:

- Data;
- Applications

Sharing is not ignoring: Monitor vendor risk continuously

Although an organisation and its cloud services provider share responsibilities, the end result is that the organisation must treat the provider as a vendor. For example, organisations running a PaaS deployment are not responsible for developing a secure server. Organisations need to treat their PaaS providers as vendors, however, and incorporate them into their vendor risk monitoring programmes.

The 'shared but not really shared' responsibility leads to confusion. As more organisations move to cloud-first or cloud-only models, they need to remember that they do not divest themselves of their privacy compliance responsibilities, they simply shift them.

SaaS will remain the largest market segment, which is forecast to grow to US$116bn next year due to the scalability of subscription-based software (see Table 1). The second-largest market segment is cloud system infrastructure services, or IaaS, which will reach US$50bn in 2020. IaaS is forecast to grow 24 per cent year over year, which is the highest growth rate across all market segments. This growth is attributed to the demands of modern applications and workloads, which require infrastructure that traditional data centres cannot meet.

TRANSFORMING KEY PERFORMANCE INDICATORS AT THE SPEED OF CLOUD

As organisations scale their cloud migration strategies, they need to establish key performance indicators (KPIs) that match the new risks. On-premises KPIs provided insight into how IT departments managed the digital assets. In the cloud, organisations need to incorporate similar KPIs but apply them to their cloud services providers in new ways.

System availability

In on-premises-only deployments, system availability referred to hardware the organisation owned. Thus, this KPI gave insight into how well IT departments managed the systems. If an on-premises

Table 1: Worldwide public cloud service revenue forecast (billions of US dollars)

	2018	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	41.7	43.7	46.9	50.2	53.8
Cloud Application Infrastructure Services (PaaS)	26.4	32.2	39.7	48.3	58.0
Cloud Application Services (SaaS)	85.7	99.5	116.0	133.0	151.1
Cloud Management and Security Services	10.5	12.0	13.8	15.7	17.6
Cloud System Infrastructure Services (IaaS)	32.4	40.3	50.0	61.3	174.1
Total Market	**196.7**	**227.8**	**266.4**	**308.5**	**354.6**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; Saas = software as a service
Note: Totals may not add up due to rounding.
Source: Gartner (November 2019)

server failed, it reflected negatively on the IT department's ability to manage upgrades appropriately.

In a cloud deployment, system availability becomes a cloud services provider vendor monitoring project. Since the cloud services provider manages the hardware and cloud server, the organisation needs to consider vulnerability to distributed denial of service (DDoS) attacks. As part of monitoring, organisations can shift their system availability KPI to monitoring IP reputation using honeypots or sinkholes.

Mean time to identify (MTTI)

On-premises MTTI metrics analysed how rapidly IT departments identified operational outages from issues such as degraded performance of hardware or software.

In the cloud, organisations can apply a similar KPI while updating it to meet cloud shared responsibility. As part of monitoring cloud services providers, organisations need to shift their MTTI KPI to focus on networks and external security controls such as domain name system (DNS) health or application security. They need to provide their IT staff with the appropriate resources for receiving alerts that incorporate the organisation's control weaknesses as well as alerts for their cloud services providers' weaknesses. Obtaining real-time alerts as part of a robust continuous monitoring compliance strategy provides an effective MTTI over discovering security vulnerabilities and provides a compliance metric for both the organisation's privacy programme and its vendor risk management programme.

Mean time to remediate (MTTR)

MTTR takes the identification KPI and provides visibility into the time it takes to respond to the identified problem. In on-premises-only deployments, this KPI gave visibility into IT help desk response times.

Leveraging this KPI for the cloud means tracking the IT and security teams' abilities to respond to identified control weaknesses. For example, MTTR should monitor patching cadence and endpoint security. Applying this to cloud service providers means monitoring the endpoints they connect to the organisation's cloud and ensuring that the service provider applies the appropriate security patches within a specified time. Organisations also need to address their own devices and software, such as application and operating system security patch updates.

With the right resources, organisations can track how long it takes their IT staff and vendors to respond to security risk alerts, giving them a key metric for proving governance over their privacy programme.

Vendor risk management

Providing KPIs for vendor risk management also moves away from traditional measurements. Self-assessment questionnaires, external audits and security operations centre (SOC) reports provide point-in-time measurements for vendor privacy controls. As malicious actors continuously evolve their attack methodologies, organisations need a more agile approach to compliance.

Managing supply chain security risk as part of an organisation's compliance KPIs requires documentation over continuous monitoring. To ensure compliance, companies need to look for real-time, automated solutions that provide the same types of reports for vendors that they use to manage their own risk.

SOC reporting and continuous monitoring/ compliance

The Certified Information Systems Auditor (CISA) manual includes a discussion on why AI use for continuous monitoring can be considered independent, or whether expanding that technology is opinion agnostic and so provides the information/ metrics but lacks the subjective quality. If used correctly, automated solutions are more objective measurements of scope as well, because if you are using them to continuously monitor everything, you are not falling into the subjective aspect of scoping an audit which can be a fundamental human error risk associated with point-in-time in SOC.

AUTOMATE FOR OPTIMAL EFFICIENCY AND EFFECTIVENESS

Optimising efficiency and effectiveness reduces the operational costs associated with compliance. From mitigating data security risk to bringing together stakeholders, automated services enable organisations to better manage all the compliance tasks needed to create a holistic privacy compliance programme.

According to the 2019 IBM 'Cost of a Data Breach' report, automating security activities with artificial intelligence, machine learning, analytics and automated incident response orchestration significantly reduced post-incident costs. Costs for organisations without security automation deployments were 95 per cent more than costs for those with automation.[15] Understanding the underlying reasons for this provides more insight into the daily operational value of these deployments as well as the overarching way they solve privacy compliance concerns.

More data, less risk

Manual processes increase compliance costs. In a 2018 McKinsey article, one cyber risk professional explained: 'we spend half our time looking for data and aggregating information from different sources'.[16] As organisations add new technologies to their IT ecosystems, they increase the amount of data necessary for appropriately analysing risk and ensuring compliance.

Additionally, manual processes and disconnected compliance information resources increase human error risk. With security information residing in multiple siloed locations, manual processes increase the risk that compliance and risk professionals will not know the information exists.

Automation provides real-time risk visibility and aggregates it in a single location to reduce the time required for gathering information. Creating a single source of documentation also ensures that all stakeholders have access to the information necessary to complete compliance tasks, ensuring better data collection and analysis.

Continuous monitoring

Privacy regulations insist that organisations comply with continuous monitoring provisions, implying that organisations need

to adopt real-time monitoring technologies to prove governance. Automation that aggregates data from across the enterprise IT ecosystem offers more effective monitoring by reducing the potential visibility issues that come from multiple monitoring locations, ultimately leading to stronger audit outcomes. Automation enables organisations to define their MTTI as they move towards a data-driven compliance approach.

Continuous documentation

From the audit perspective, organisations need to document their monitoring activities. With automated solutions that track both the monitoring and the mitigation activities, organisations can better define their MTTR, track the time it takes for their IT departments and vendors to respond to alerts, and prove their governance. Documenting activities reduces audit costs arising from auditors interviewing staff members, provides independent data over vendor risk monitoring and establishes data-driven KPI so organisations can continuously improve their compliance posture.

Continuous assurance

Bringing together continuous monitoring with continuous documentation capabilities gives organisations a way to create a compliance programme that incorporates continuous assurance. They can leverage their continuous assurance in several ways. First, they can provide upstream supply chain partners confidence over their privacy controls, easing their customers' vendor risk management processes and accelerating the sales cycle. Second, they streamline their audit documentation gathering processes to reduce audit costs. Third, by creating a continuous assurance approach to privacy compliance, they more effectively communicate with internal stakeholders. As more privacy regulations require board of directors oversight, a continuous assurance posture eases burdens associated with these new controls.

DATA-DRIVEN CONTINUOUS ASSURANCE FOR CLOUD PRIVACY COMPLIANCE

Committing to a data-driven continuous assurance privacy programme provides a more robust compliance posture. As organisations build out their digital transformation strategies, they need to think strategically about the way in which they manage privacy compliance in the cloud.

The first step to creating a data-driven continuous assurance programme is to assign responsibilities by identifying key organisational stakeholders and the metrics they need. IT and compliance officers may both need to monitor cloud risks, but they also need different information to fulfil their job functions. Managing privacy compliance in the cloud needs to incorporate all users as organisations build out their technology adoption strategies.

After building the privacy compliance team, organisations should create a team-based approach to analysing risk, reporting effectiveness, responding to threats and continuously updating their programme. Organisations need all stakeholders to buy into the programme while also finding a way to meet divergent needs. Creating an overarching approach that begins with risk analysis and ends with continuous improvement requires the right data for the right people. As part of the data-driven continuous assurance approach, organisations need to define the KPIs that prove effectiveness and drive improvement.

In an IT landscape rapidly evolving from 'trust but verify' to 'trust no one', communication will be the key driver for privacy compliance initiatives. Continuous assurance that intrinsically incorporates key metrics can help drive organisations to not only adopt the appropriate controls but ensure that they remain appropriate over time.

References

1. Gartner (November 2019), 'Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020', Gartner, available at https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020 (accessed 28th July, 2020).
2. Stoudt-Hansen, S., Karamouzis, F., Villa, A., Ray, S., Dunie, R., Sturgill, N., Shotton, L., Miers, D. and Biscotti, F. (December 2019), 'Predicts 2020: RPA Renaissance Driven by Morphing Offerings and Zeal for Operational Excellence', Gartner, available at https://www.gartner.com/doc/reprints?id=1-1Y5AZSMA&ct=200116&st=sb&__hssc=71912524.1.1584559952706&__hstc=71912524.33798a27280ecf480418a37425822076.1584559952706.1584559952706.1584559952706.1&__hsfp=2216057658&hsCtaTracking=841753c0-ca8b-4a19-9d00-0de5b09847e4%7Cd86385d9-4454-4901-ac6e-dd3ae9feab30 (accessed 28th July, 2020).
3. Check Point, 'The 2019 Security Report', available at https://www.cloudcomputing-news.net/news/2019/feb/22/check-point-exposes-yet-more-shared-responsibility-misunderstandings-cloud-security/ (accessed 28th July, 2020).
4. Security Scorecard (March 2019), 'Looking Ahead to RSAC 2019: How Can We Work for BETTER Privacy and Security?', available at https://securityscorecard.com/blog/looking-ahead-to-rsac-2019 (accessed 28th July, 2020).
5. Syntonic Research (March 2019), 'BYOD Policy Requirements for a Secure BYOD Environment', available at https://solutions.pcmcanada.com/byod-policy-requirements-for-a-secure-byod-environment (accessed 28th July, 2020).
6. Boufis, E. (January 2019), 'Profit, Peril and the Internet of Things', *Forbes*, available at https://www.forbes.com/sites/eliboufis/2019/01/02/profit-peril-and-the- internet-of-things (accessed 28th July, 2020).
7. Lemos, R. (March 2019), 'New IoT Security Bill: Third Time's the Charm?', DarkReading, available at https://www.darkreading.com/iot/new-iot-security-bill-third-times-the-charm/d/d-id/1334190 (accessed 28th July, 2020).
8. ISC2 (February 2020), 'Breaches Increased in 2019, But the Number of Exposed Records Declined', available at https://blog.isc2.org/isc2_blog/2020/02/breaches-increased-in-2019-but-the-number-of-exposed-records-declined.html (accessed 28th July, 2020).
9. Privacy Affairs (March 2020), 'GDPR Fines Tracker & Statistics', available at https://www.privacyaffairs.com/gdpr-fines/ (accessed 28th July, 2020).
10. National Institute of Standards and Technology (2020)' 'Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management', available at https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf (accessed 28th July, 2020).
11. NetDilligence (2019), 'Cyber Claims Study 2019 Report', available at https://netdiligence.com/wp-content/uploads/2019/10/2019_NetD_Claims_Study_Report_1.1.pdf (accessed 28th July, 2020).
12. Panetta, K. (October 2019), 'Is the Cloud Secure?', Gartner, available at https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/ (accessed 28th July, 2020).
13. Oracle and KPMG (2019). 'Oracle and KPMG Cloud Threat Report 2019', Oracle, available at https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf?elqTrackId=063c9f4a2a5b465ab55b734007a900f0&elqaid=79797&elqat=2 (accessed 28th July, 2020).
14. McAfee (2019), 'Cloud Adoption Risk Report 2019', available at https://cloudsecurity.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf (accessed 28th July, 2020).
15. IBM Security (2019), 'Cost of a Data Breach', available at https://www.ibm.com/security/data-breach (accessed 28th July, 2020).
16. Boehm, J., Merrath, P., Poppensieker T., Riemenschnitter, R. and Stähle, T. (November 2018), 'Cyber risk measurement and the holistic cybersecurity approach', McKinsey, available at https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach (accessed 28th July, 2020).