Remarks of Dorian Daley, Executive Vice President and General Counsel of Oracle Corporation
prepared for and given at the
Thought Leadership Event on Big Data and Data Privacy and Security
hosted by
The Central Bank of Kenya at the Kenya School of Monetary Studies
21 March 2019

Asante sana, Governor Njoroge, and thank you Deputy Governor Mbijjewe as well. I am most honored to be here at your invitation. And I am thrilled to be back in Kenya. This is my 4th trip to the country and 5th to the region in the last 10 years, and it is a place that I always look forward to for its beauty and the warmth, energy and innovative spirit of its people, including my very talented team here with me today. By the way, I should note that they just yesterday gave me a new name – a Kenyan name : Nyaguthii. I understand this means, "on the go" or "traveler", which apparently I have earned for my many travels.

Before I begin, let me say to any attendees here today from Mozambique, Zimbabwe or Malawi, my heart – I'm sure all our hearts – go out to you and to your people following this week's tragedy. You are in our thoughts and prayers.

It is not uncommon that when I show up at work to speak to a large audience, it makes people nervous. It's not personal, the trepidation attaches to my role as an attorney, a senior executive and the chief legal officer of the company, and the head of our compliance and ethics program and team.

But I confess that the tables are turned here today, and I am in fact the one who is a bit nervous. Speaking to a room full of bankers – sophisticated financial services executives and officials – is not in my wheelhouse. You all have a type of expertise that I do not share. I admire it, for sure, but I do not share it. Your responsibilities are great and far ranging. Your national economies, and indeed the social fabric of your countries, depend on you.

But I have reflected on things we do share:
We are highly trained and educated.
We value continuous learning and professional evolution.
We run large organizations with high impact and we have large customer bases.
We have a parallel desire for stability *and* innovation, which necessarily implies change, often rapid change, in order to meet new challenges and provide better service.
We have a drive to be better today than we were yesterday.
We have the professional commitment to improve lives and contribute to the common good of our communities and our countries.
And we have a commitment to ethics and integrity in our business conduct.

So I am feeling better…a little less intimidated.

And I'm delighted to speak with you today on a topic that touches on many of these shared values, goals, and experiences. Namely:

1) The value and opportunity of the use of data – LOTS of data – to improve and expand the functioning of your organizations and the services you provide, and

2) Ensuring that the technologies used, and the policies and practices and protocols employed collect and use large amounts of data, will protect that data – from both a privacy and security perspective – AND protect the overall financial systems on which the commerce and the stability of the region depends.

I pledge to you at the outset, this will not be a technical discussion. After all, I am a lawyer - not a software or hardware engineer.

The Economist magazine has likened data in this century to what oil was in the last one: "A driver of growth and change" creating new infrastructures, businesses, economics, and even politics, and requiring changing rules for markets and new approaches from regulators. According to the McKinsey Global Institute, data driven organizations are 23 times more likely to acquire customers, 6 times more likely to retain those customers, and 19 times more likely to be profitable as a result. And industry analyst IDC predicts that data driven organizations will have a $430 billion advantage over their rivals by next year.

So there is no question that data is the new, and a very valuable, currency of commerce.

The amount of data is skyrocketing. We create data from every action and interaction, creating a kind of a data-network effect, where data simply tends to create more data. Some recent estimates claim that approximately 90% of all data worldwide today has been generated in just the last 5 years. IDC predicts that the amount of data created and copied every year will reach 44 zetabytes next year and 180 zetabytes by 2025. And if you are like me and don't deal in zetabytes, that's a number with 21 zeros after it.

The type and quality of the data is also changing dramatically. We have gone from relatively limited amounts of structured data (think age, address, gender) to vast amounts of unstructured data, known as "big data" (think of the data created by social interactions, shopping habits, travel or location, and data generated by literally thousands of different kinds of devices, from washing machines to cars to thermostats).

And the value of all that data is increasing. How? How is it that all this unrelated data can be mined, selected, sorted and made useful? How do we get beyond what is estimated to be only a tiny fraction of this data being analyzed and leveraged?

The answer is through sophisticated data analytics tools, including the use of artificial intelligence and machine learning technologies.

The goal of these technologies, broadly speaking, is to create thinking machines. They are "artificial" only in the sense that the tasks are not performed by human thought, but they are based on *real* data. Machine learning – an important subset of AI for data analytics – uses mathematical algorithms to perform a task by looking for patterns in data, drawing inferences, and then continuing to learn from new data. The more data, the better the outcome of the task performed. A computer system using machine learning can progressively improve its own performance by creating new algorithms from these large volumes of data.

In my own company and in many others, we call these adaptive intelligent apps (or applications). They are adaptive because they learn from user behavior and react and optimize in real time. And they are intelligent in that they derive insights from the data to deliver better, more accurate outcomes.

Let me give two examples. First, in the tech world, Tesla cars collect enormous amounts of data and data is used to enable the optimization of the self driving technology, which in turn updates the cars' software automatically. Second, in the world of manufacturing, GE developed a new operating system to help its customers control their GE machinery. The system is essentially a giant data collections system where data is pulled from a variety of sources and algorithms are created and trained to improve the operation of that machinery.

Ok, so data – big data – is a valuable currency that can be mined, mixed, analyzed, and leveraged through AI and machine learning to obtain insights in order to improve operations and services and create new services and markets. What does that mean for the financial services sector? It turns out, it means quite a lot. But before I dive into how these big data crunching technologies can benefit your industry specifically, I'd like to first note what I've come to think of as fundamental tenants regarding that journey into this new data economy, because I think they provide important guideposts for embarking on any project to take advantage of all this data you have and can get: SIMPLIFY, INNOVATE, DEFINE THE PROBLEM, GOAL SETTING, DON'T LOSE TRACK, SECURITY, LEADERSHIP. Please allow me to explain briefly.

SIMPLIFY your information management platform so that it is scalable and elastic, and demand flexibility so that it will meet ever more stringent regulations *and* you can identify and incorporate disparate sources of data within a timescale to change outcomes and increase value.

INNOVATE not just with new technology, but by changing the *way* you work, up and down the chain, to take advantage of these tools to harness the power of your data. Changing the mindset of the entire organization is important.

KNOW WHAT PROBLEM YOU ARE TRYING TO SOLVE. In the financial services sector we have seen the full gamut of problems or challenges: a lack of unified sources of information, insufficient data, an inability to collaborate, aged legacy systems, redundant and inefficient processes, silo'd systems, fragmented analyses, limited risk adjusted performance capabilities,

inefficient modeling and stress testing, long close cycles, inflexible and duplicative tools, lack of transparency, and insufficient controls – all these create risk: Risks impacting accurate and timely reconciliations, risks impacting statutory and regulatory compliance, risks related to competitiveness and stability in the market, and risks related to cybercrime and fraud.

SET CLEAR GOALS. And here the purpose ought to be to create real value by moving from using analytics to merely serve up information, to using these tools for automated decision making, execution, and control capabilities. And think expansively about how you can share and trade information within your ecosystem where it is permitted.

DON'T LOSE TRACK OF THE BIG DATA FOREST FOR THE TREES. The core proposition of the big data strategy is to analyze combined data sources to increase its overall value, but context matters. So losing sight of where the data comes from can negatively impact the ability to assess its relevance in the new context. Additionally, like all of us humans, data ages, so it must be updated to ensure its relevance.

SECURITY IS KEY. Securing the data from a systems and access perspective is a critical priority. More on that momentarily.

And finally, **THE JOURNEY TAKES LEADERSHIP,** vision. This is what you are called upon to demonstrate every day. Leadership and vision as I have seen with the Governor and Deputy Governor of the Central Bank here is one of the most important prerequisites to the journey. It is a big, bold step, impacting the entire organization. Without strong executive leadership, vision, and commitment to get everyone not only on the same page as to priorities and tasks, but with respect to the imperative and the exciting opportunity the journey can yield, progress simply cannot be achieved.

We and many other technology vendors have been in Africa for some time now, engaging with the financial services industry and central banks as main drivers in their economies, and what we observe as drivers for further modernization will come as no surprise to you. Financial institutions across the board are maturing rapidly and seeing increased competition, including from non-traditional banking services. Regulation is increasing, and the cost of regulatory compliance is high. Institutions within the financial services ecosystem are seeking out a more sophisticated framework and proces***s*** for interactions. Institutions seek to grow and expand services, but also seek stability. More effectively fighting cybercrime and fraud is an imperative. And aged legacy systems threaten innovation and productivity, with some having hardware components that are being phased out or are not at all equipped to tap into large amounts of unstructured data.

The Central Banks in the region have additional drivers due to their multifaceted responsibilities as banker AND economic advisor to their governments, prudential regulatory authority (including over disruptive "fintech" entrants to the market), financial markets and reserve management, formulation of monetary policy and operations, and much more.

And core to any Central Bank mission is building that relationship of "mutual trust" with its constituent financial institutions through regular open communication in order to "foster a stable banking sector" and "sustainable growth in the economy."

So…much is at stake.

The potential benefits of a modernized, intelligent system to take advantage of the wealth of big data are concrete and many. The heads of many Central Banks, including Jerome Powell in the U.S., Mark Carney in the U.K., Lesetja Kganyago of South Africa and our esteemed host, Dr. Patrick Njoroge, have all embraced the value of data to Central Bank operations and policies. The external benefits of improved reporting and analytical capabilities can have a positive impact on the management of inflation, interest rates, debt, and exchange rates, which in turn can help grow GDP and reduce unemployment.

Broadly speaking, the benefits to any organization in the sector are many. Improved operational efficiency can improve reporting at all levels, but also improve internal communications, enhance worker productivity, eliminate human error and delays through automated decision making, and dramatically reduce IT costs.

In lending, some estimates suggest that lenders often collect a relatively small number of data points about a borrower when making a lending decision. Big data can help bring hundreds or even thousands of data points about a borrower, which helps make much more informed decisions. And what can take significant time and effort for humans to research and assess, can be assembled and processed almost instantaneously by an algorithm. For consumer loans, a frequent method of assessing someone's risk in many countries is through a credit score. But these are often not available, leaving too many people unable to be qualified. So one particularly rich source of data now being used to assess creditworthiness and risk is the data from mobile phone app use, which can reach many more people in a given market. Big data can also help institutions assess their own health in lending by identifying and evaluating factors related to their own financial position that should be considered before making a particularly large lending decision. This can include information about the current economy or economies in which the institution operates, macro lending trends, current levels of capital available for investment, the customer's location, what industry the customer is in, and much more.

Big data also dramatically expands the information available to analysts at financial services firms when they make investment decisions. This information can be used for both investing an organization's own funds, as well as for providing investment advice to clients. This data can include not only the public financial information about a company's earnings and overall performance, but also all of the recent news stories about the company, social and political trends in the countries or regions where the company is located, and even whether the company is trending on social media. All of this can provide insight into the future health and profitability of the company that can help inform investment decisions or advice to clients.

The benefit to the customer or consumer is enhanced in many other ways, as well. Communications improve through a continuous feedback loop from mobile devices; existing products and services are enhanced and new ones created, tailored to customer preferences based on customer insights derived from the data. This potential for customer insights is huge, allowing for a 360 degree view across the entire customer lifecycle through sentiment analysis and viewing client behavior patterns. This, and profitability analyses across customer segments, and analysis of marketing activity on customer engagement, can drive tremendous cross sell and up sell opportunities. AI and big data are changing online marketing itself in dramatic ways, allowing for targeted ads to consumers who are more likely to be interested in specific financial products.

And all of this analysis of big data through AI and machine learning can also allow for detection of anomalies to help combat fraud.

The fight against financial crimes and money laundering is raging. The reported rate of economic crimes worldwide is increasing, and in Kenya, for example, fraud committed by the consumer is the second most prevalent economic crime. The costs of compliance to combat fraud and money laundering have been high, due to the time intensive manual investigative processes used; the high volumes of false positives from present detection systems; disparate and unconnected data sources; and the inability to detect patterns, relationships and links across entities.

Hence, financial institutions are increasingly moving toward automation of repeatable tasks and machine learning based systems to apply state of the art detection logic to transaction monitoring. This is done through the data collection, correlation, and entity linking across multiple data sources such as: internal and external watch lists; customer account, product and transaction histories; and information from correspondent banks, beneficiaries, originators, intermediaries, remitters, government and law enforcement.

As Bill Winters, CEO of Standard Chartered, wrote in an op ed in the Financial Times last year, “New machine learning technologies will allow financial institutions to evaluate vast quantities of data more quickly and fine tune our surveillance tools.” And, he added, “Regulatory support for these innovations is vital…”

The monitoring, detection and mitigation of cybersecurity threats has become extremely sophisticated, whether those threats come in through spam, malicious code or via malicious websites or other sources. At the database level AI and machine learning technologies are being employed to allow the provisioning, security, monitoring, backup, recovery, tuning and troubleshooting of the database without human involvement, as well as automatic patching and upgrades, all while running. And “bot managers” (essentially mini robots) can be deployed to analyze website traffic in real time to automatically classify threats and then activate countermeasures to block incoming non-human (that is, malicious botnet) traffic, selecting the countermeasure depending on the sophistication of the malicious botnet. It’s high drama in the fight against cybercrime, and it is done automatically.

Of course, with all this opportunity comes challenges and a new set of risks, and by this I mean risks around data privacy and security.

In order to understand the different risks related to data privacy and data security, it is important to remember how different these two concepts are. Data security is strictly about protecting the confidentiality, integrity and availability of information, whether it is in electronic form or in hard copy. And it can be any type of data asset: intellectual property, trade secrets, customer information, personal information, financial performance data, or future business plans, for example. Data needs to be protected on the systems and networks where it is stored, as well as from the people who may physically access those systems and networks. So while data security is vastly complex technically in terms of how it is managed, the concept is quite straightforward: keep it secure from unauthorized access.

In contrast, data privacy is a single concept that has many different components. Security is one of them, because you cannot keep your data private if it is not secured. But there are other concepts, such as: limiting use; minimizing collection; providing notice, choice and access; being transparent and accountable; and keeping data accurate and up to date.

Because data security and data privacy are quite different, the risks related to them are as well. So permit me to address them in turn.

Data Security Risk is divided into two worlds: unauthorized access from external actors, and unauthorized access from those within your organization. Both are destructive. Most of the attention gets focused on external actors, because they intuitively feel more threatening: hackers, cybercriminals and terrorists are trying to penetrate your systems and steal your data, and sometimes they are state sponsored and the intent is to advance geopolitical interests. But in fact, most security incidents are a result of actions taken by internal employees and contractors. And these can run the gamut from a disgruntled employee trying to damage his or her employer to someone acting on an ideological agenda like Edward Snowden.

The risks posed to organizations from a breach of data security have now become intuitive to us, because we see them in the news almost every day. For example:

- When a large amount of personal information is compromised, consumers can be injured by identity theft and loss of time and money in restoring financial credit.
- Many companies store or manage data on behalf of their customers. If the integrity of that data is compromised, it can have a material negative financial impact on that customer, both in terms of the customer's operations as well as its regulatory requirements.
- By losing the operation of its website, or interruption to the availability of data, or if the breach results in the loss of money from fraudulent fund transfers, security incidents

can have a material financial cost to the organization, and a significant impact on operations as the organization labors to remediate the effects of the attack.

- There are often ancillary monetary damages suffered by entities such as credit card issuing banks.
- Brand and reputation damage can follow when systems are breached, even when the breach is caused by highly sophisticated criminals who manage to penetrate those systems despite an excellent security program.
- And in some cases, national security may be put at risk if information necessary for the operation of governmental functions and a country's critical infrastructure is damaged or permanently compromised.

Despite all these significant dangers, business must go on. Access and use of data is simply critical to the operation of the global economy and the delivery of goods and services. This is why most companies take a risk based approach to security, paying particular attention to the large data sets and the most sensitive data. This means creating a holistic security program. I'll get to a description of the security policies and practices that from my perspective are the most important parts of such a program, but first, I want to share some thoughts on privacy risk as well.

Data Privacy Risks are associated with the distinct concepts that together make up data privacy rights, as set forth in various legal regimes: use, minimizing collection, notice, choice, access, transparency, accountability, accuracy and security. I've outlined the security risks, so let me quickly address each of the other privacy risks before turning to the general global regulatory frameworks governing the processing of personal information, which impose these concepts as legal requirements in different ways and to different degrees.

Limitations on the use of data - this can be a challenge to manage. Entities generally collect information for either a very specific purpose or a fairly defined set of purposes. You know why you want to use it because you are collecting it, and generally you don't bother collecting something for no reason. That is pretty intuitive. The challenge is that possible uses of data may change over time. What was a limited use case in 2009 may seem overly constricting in 2019. In addition, given the expanding possibilities that big data and artificial intelligence are now providing, it is likely that organizations will want to use data in new and novel ways not foreseen at the time of collection. This debate played out in the drafting of global privacy regulations, as regulators acknowledged that being constrained in the uses of data may not be in the interests of either the individual or the organization that collected it. Aside from exceptions like public research or public safety, more regulators are signaling the ability to use data in manners consistent with the initial use, even if not identical. But a risk analysis should performed whenever an organization wants to use data in very new and novel ways.

With respect to **minimizing data collection**, the game has changed here, with the dramatic drop in storage and computing costs and the rise of big data. Previously, entities were incented only to collect data that was necessary for the purpose they were collecting it for. The interests of the individual and the organizations collecting the data were aligned. Big data and machine

learning has changed that, as more data means more insights and more possibilities for use. Nonetheless, it is important to be aware of and comply with applicable data minimization requirements.

When providing **notice** to individuals about how their data will be handled, it is important that it is an accurate description. Otherwise, the individual who provides the data will not be deemed to have appropriately been informed of the uses, which can undermine your right to use that data.

The concept of **choice** recognizes that individuals should have some input in how entities use their personal information. While there are some exceptions where handling a particular data element is absolutely necessary (such as collecting government identifiers from employees in the employment context), in most cases, laws provide for individuals to exercise some degree of control over their information. It is therefore important for organizations to know where personal information is stored and used. If an individual exercises choice by opting out of his or her data being used, that opt out needs flow through to all repositories where that data may reside.

Access is a right designed to ensure that individuals can see what data an entity has about them, with the ability to exercise their choice to opt out. While access is not an unlimited right in most legal regimes, it can still be challenging to develop processes designed to provide this access and costly to implement.

Transparency is rooted in the concept that individuals should be able to understand how an entity is using their data. Generally, this requirement is addressed by a privacy notice, which describes what types of personal information an organization collects, how it is used, how it is shared, how long it is retained, how to exercise choice, and who to contact with questions. This information must be accurate and complete so the individual is deemed to understand and agree to the processing. Changing this notice is necessary as soon as an organization identifies a different use case or implements significant changes to its data handling practices.

And finally, an organization needs to hold its employees and contractors **accountable** for their handling of personal information, in a manner consistent with the organization's privacy obligations. It is very important that the individuals understand this obligation, because the organization may be held accountable by regulators for their failures.

How these privacy principles will be applied depends on industry regulators, or the national laws of the country in which an organization operates, or the laws of the jurisdiction in which an entity does business and collects personal information.

And this global privacy regulatory framework is evolving at lightning speed. Traditionally, countries have taken one of two approaches. The first approach, which was adopted by European countries, was to treat privacy as a fundamental right under the law. This approach defined personal information broadly and imposed specific process requirements on its

handling. Notably, it also imposed restrictions on the movement of that information only to countries who could meet those specific requirements. The second approach, which was adopted by the United States, was to treat privacy as applying to specific data in certain contexts, such as consumer financial information or health information. These laws did not impose limitations on the movement of personal information globally as long as the controls applicable to the data were applied whenever the data was accessed.

Over time, many countries in Africa, Asia, and South America adopted privacy laws generally taking one or the other approach. That process has accelerated and changed significantly with the passage of the European Union's General Data Protection Regulation, or GDPR, which came into full effect in May of 2018. The countries considering new privacy laws or updating their existing laws are all focused on alignment with the GDPR.

Kenya enshrined the right to privacy as a constitutional right back in its 2010 Constitution and has existing laws and regulatory guidance to ensure the right of access, criminalize unauthorized access and computer misuse (though certain sections of this act are under high court review), prevent telecommunications service providers from intercepting or disclosing subscriber information, require banks to maintain confidentiality of customer information and establish adequate governance mechanisms, and maintain the confidentiality of health information.

Kenya is also considering new data privacy legislation with a draft bill that is broadly consistent with the GDPR. The initial Kenyan draft bill also contained limitations on access or storage of data outside of Kenya, which is also referred to as "data localization." These requirements have not been implemented under most privacy laws, including the GDPR. While requiring data to be stored in-country gives governments direct physical access to the personal information related to its citizens, it does come with some cost. Local facilities may not be able provide the best security available globally. Security is not necessarily solved by keeping the data local. Additionally, software vendors are not always able to staff product expertise on a country by country basis, but instead do so on a global basis. This can slow the remediation of a problem where personal data must be accessed to solve the problem. And finally, global providers are able to leverage global cost structures to reduce overall costs.

As you might expect, a technology company believes that security risks from cross border flows can be addressed by other technologies such as encryption and tokenization rather than data localization. While the current draft of the Kenyan data privacy bill maintains the outright prohibition on cross border transfers of "sensitive" personal data, it allows it for other personal data with the consent of the data subject and on obtaining confirmation of appropriate safeguards. Sensitive personal data is defined broadly, however, and includes data that can reveal the race, health status, ethnic social origin, political opinions, religious beliefs, personal preferences, location, genetic data, biometrics, sex life or orientation, or personal financial expenditures of the data subject.

As has now become quite clear, one of the greatest risks related to privacy regulation is just the sheer number of global privacy laws that may apply to data being used by an organization. As pointed out by Deloitte in its overview of data protection and privacy laws across the African continent, "there is no unified approach" and "adapting personal data compliance programs to address disparate legislation and regulation is no minor feat." It is an extremely complex process to track what controls should apply to what data, what terms should be applied to contractors and suppliers, how intracompany agreements should be structured to enable the global flow of data where possible, and whether system segregation or other nonstandard processes are required.

But sophisticated global data privacy compliance programs are both necessary and here to stay. The GDPR sets forth a maximum penalty for violations of 4% of an organization's global revenues, and other countries are following suit with fines or jail time. So there is a very strong incentive to comply, in addition to the desire to maintain the trust of our customers, as vigilant stewards of their personal information.

Because security has been core to my own company's mission since its inception, this focus on security and privacy was not new to us. We have learned a lot in our 42 years of business… and a dramatic amount in just the last 5 years, with a full court press in preparation for the GDPR compliance deadline. One benefit is that GDPR did bring an overall organizational clarity to the process, with clearly defined responsibilities down through the various lines of business, such that there is little question but that ensuring privacy and security is the responsibility of everyone in the organization – not just the lawyers, not just the information security professionals - everyone.

The approach that we advocate is a combination of: policies, practices and protocols combined with the important technologies that can protect data, including cloud computing technology; a perspective that our program is a living, breathing thing that must continually evolve and improve over time; and a program of education, training and accountability that never ends. I'd like to turn to some of these best practices next.

While it may sound like a lawyerly thing to say, the development and implementation of clear policies, and training regarding those policies, is the foundation of any privacy and security compliance program.

A **Privacy policy** should cover all aspects of the organization's handling of the personal information it collects to ensure that it has the rights to use the data for its intended purposes, is transparent in its operations, and has the required processes to enable individuals to exercise any rights they may have under the law. It has to speak in plain language – that is, not as though it is written by a lawyer.

A Data classification policy is important because not all data used by an organization is of equal sensitivity. Some of it is personal information, but most of it is business data. A policy that classifies all data into different levels of sensitivity can guide employees and contractors on how

to handle the different types of data. Appropriate restrictions on access, (including sharing internally and externally), and other specific handling requirements (like encryption) can then be specified depending on the sensitivity classification. Generally, organizations choose at least three levels of sensitivity, such as Public, Confidential, and Highly Confidential.

An Acceptable use policy relates to employees' use of internal, third party, or in some cases personal systems and resources to access, collect, use, store, and share information about an organization's business and its employees, customers, and suppliers. An acceptable use policy should provide guidance on which technologies are appropriate for use, and which are not, given the security risk that they may pose. This includes usage of technologies like email, messaging applications, mobile devices, third party storage systems, video conferencing, encryption technologies, and much more.

A Security incident response policy should guide employees on all aspects of incident response. That means establishing guidelines on how to report an incident to the organization's information security group as soon as it is suspected to have occurred, who manages the incident, how communications are drafted and approved, and how the legal team is engaged to assess any notification responsibilities. An incident response team should be created with specific responsibilities assigned.

Recognizing that most employees use some kind of computing device for work purposes, organizations should develop a **hardware security policy** to set basic standards for the security controls that apply to mobile devices, laptops, desktops, and servers. This may include use of encryption, firewalls, anti-virus software, security updates, patching, hardening, logging, and end of life disposal. The more automated many of these functions are, the better.

And it is critical that enterprises also set minimum standards for **passwords**, as you would be surprised how often passwords are hacked or compromised due just to poor password hygiene. The standards should apply in all contexts, whether the password applies to access to a laptop, a network, or a server. The growth of computing power has opened up a whole new avenue for attackers as they brute-force attack systems trying to generate the password. Simple passwords have no chance of surviving these attacks. Systems should force PW changes regularly, and shared or generic passwords should really never be used.

These core policies are an important way to establish a baseline standard for operations across the company and enforce them if not followed. There are other security policies that organizations may consider adopting. But we also need to be sensitive to policy fatigue, where there are just so many policies to follow that employees either have a genuinely hard time following them or they will not even try. We try to strike a balance between the corporate wide policies and those operational requirements that may apply to different operational areas of the company and can be managed on that basis, rather than an enterprise-wide basis.

In addition to a strong policy framework and training around it, we advocate for an **Organizational Privacy and Security** framework that covers all avenues to data: physical security, system security and information security.

Senior executives should absolutely be involved in the oversight of the privacy and security program, with reports delivered on a periodic basis to a governing body that includes certain senior executives. This establishes a focus and a consistent approach to security throughout the organization and ensures that issues needing resolution are addressed without equivocation and in a timely manner. At my company we have the Oracle Security Oversight Committee, or OSOC, chaired by myself, one of our two CEOs, and our Chief Corporate Architect who has an expertise in product, organizational, and program security; and to whom our global information security team, physical security team and Chief Information Security Officer all report. We meet on a quarterly basis with the Chief Privacy Officer, who reports directly to me, and the leads for all security, information technology and corporate systems groups as well as internal audit and various product development groups for a half day deep dive that some participants have likened to a "corporate colonoscopy."

Additionally, establishing a cross functional system review board to enforce standards and enable review of all new systems before they go live is an invaluable tool. This review should focus on all aspects of the system being introduced, including where it is located, how it is architected, what data it will process, whether its activities are consistent with applicable internal policies, which groups internally or suppliers externally will be permitted access, and how long the data will be retained. The system should then be subject to a security technical review, including a penetration test to confirm it is secure. With this comprehensive type of review, organizations can have much greater confidence that every system meets established security standards and is processing data in accordance with its legal obligations. Anyone who tries to skirt this review will be invited to our quarterly OSOC party to explain why.

And finally, we have established a global privacy council comprised of individuals from over 40 lines of business and the internal organization privacy leads. They are responsible for implementing, documenting and maintaining processes within their lines of business as required to comply with the company's global privacy and data protection requirements. We also have appointed information security managers who are embedded in each line of business who are trained in privacy and security issues and raise matters directly with the legal team for consideration.

Best practices in security and maintaining privacy of sensitive personal information also includes a program of **Asset Classification and Control.** Clearly**,** without knowing what computing assets an organization has and who the owners of the systems are, it is impossible to maintain the security of the infrastructure. Those computing assets also need to be classified by the sensitivity of the data they process, so the appropriate controls can be applied for that data. Whether applying patches or software updates, or monitoring network activities, having unmonitored assets is like locking every door in your home but leaving the windows open. It

just takes one system having out of date software to enable an attacker to gain access to enterprise systems.

Human Resources or Human Capital Security functions are also important in the overall security scheme. The majority of all security incidents are performed by internal attackers, whether they are employees or contractors. Background screening and limiting access physically and by policy to certain sites and websites can help reduce risk, and where allowed, monitoring tools should be considered.

Employees also need to understand what their own responsibilities are when it comes to protecting the data they have access to. Training on a recurring basis should therefore be required of all employees, with supplemental training for those with access to, or who are involved in, the processing of particularly sensitive data. Automated systems can help push the mandatory training and track whether the training has been completed, with consequences for failure to get it done.

Physical security also needs to cover the ways in which individuals might be able to physically access an organization's servers or networks. These include confirming identity, recording and badging visitors and vendors, limiting access to certain areas, and preventing the use of certain devices around sensitive areas. An entire program around physical security must be built, continuously improved upon, monitored and tested.

Operations Management of the computing infrastructure, while highly complex and multi-faceted, is absolutely critical to any program. It requires management of both hardware and networks, with segregated duties so that groups only have access to the systems that they need to, and no others.

In managing hardware, computers connected to the enterprise's networks should be required to have anti-virus, firewall and desktop asset management software installed with all security updates enabled. Or to put a finer point on it, these should be configured in a way in which the security updates cannot be disabled.

When managing the network, security teams should employ intrusion prevention and detection systems to provide surveillance for intercepting and enabling rapid response to security events as they are identified.

And finally, security-related activities on operating systems, applications, databases, and network devices should always be automatically logged. It is surprising how often organizations will turn off logging. Logs should be regularly reviewed – preferably in an autonomous fashion without requiring human intervention - for forensic purposes and incidents, with any identified anomalous activities fed into the security incident management process.

Access Control is another critical component of a first class program and refers to the policies, procedures, and tools that govern the access to and use of computing resources. Examples of

resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol. Access should be enabled only those resources that are absolutely required to perform the employees' function. And it is critically important to keep the access privileges up to date, so that in the event of employee terminations, deaths or resignations, access can be terminated quickly.

An effective security program should also cover **Business Continuity and Emergency Management.** All organizations of course need to plan for interruptions to business operations and service delivery so there is clear guidance on how operations will continue in spite of potentially business-disruptive events. This also must include a plan for backup of critical data and a mechanism to prevent intrusion by bad actors trying to take advantage of the emergency and disruption.

And finally, **Privacy by Design** is something of a new concept. We and many other organizations have embraced it, and developed attendant training to help translate the privacy principles of our data protection and security policies into actionable guidance for developers and engineers. This is intended to help them create privacy features and functionality in new and upgraded products and services and to document those security features so that customers know and understand them. This in turn enables our customers to address the privacy rights of their end users.

These program components combined with foundational privacy and security policies, effective training, and the new adaptive intelligent apps that harness the power of volumes of structured and unstructured data across multiple sources to create value represent a modern and comprehensive approach to business – and banking – in the 21st century. They are part of a whole, as one without the other will not deliver exceptional value and the trust and stability this sector requires. I encourage you all to explore the benefits of this data driven economy, which can and must be done while ensuring the security of your systems, the privacy of your citizens and the stability of your sector.

Asanteni Sana.