Proactively adapting to cross-border regulatory needs

Understanding the impact of cross-border compliance requirements on controlling enterprise data access

EY
Building a better working world

Introduction

With the rapidly changing and increasing regulations for cross-border data access and protection, organizations have become more reactive rather than proactive to be in compliance.

Cross-border data protection regulations address the safe movement of personal data outside of the border of its origin. These changing regulations drive organizations to make interim changes to their existing access management and data privacy strategies – a practice that is not sustainable in the long term. Traditional methods of access management (such as entitlement or role-based access control) and protection (such as limited to data center environments, confined to single-tier protection) are not compatible with ever-changing regulatory requirements.

Why is this important?

- **Lack of awareness** regarding data protection regulations of different countries, leading to noncompliance
- Challenges to sustain an **ever-changing cyber environment**
- Increasing risk of ransomware attacks, losing customer personal information and **violations of regulatory compliance** often result in legal punishments, inquiries and federal fines
- Management with access at a granular level cannot be achieved with **traditional and siloed access and data protection controls**
- **Reliance on unscalable manual processes** when responding to data loss incidents and reports, leading to delays and causing severe loss of customer trust and market reputation

Who is this paper for?

- Chief information security officers (CISOs)
- Chief information officers (CIOs)
- Chief innovation officers (CIOs)
- Chief digital officers (CDOs)
- Customer-facing product owners
- Identity owners business-to-business (B2B), business-to-employee (B2E), business-to-customer (B2C)
- Data privacy officers (DPOs)
- Security architects

What are cross-border restrictions and their impact on cyber controls?

Data privacy compliance requirements

Data localization regulations are strict and require organizations to use, store or process data in the country of its origin. Countries like Australia, the United Kingdom and China, as well as regions like Europe have local regulations to not only store and process personal data within borders but also to restrict access to people outside of those individual regions. To apply access restrictions, organizations first identify which country the data is from and who outside of that country has access to the data. In such cases, **identification and collection of data location becomes challenging due to manual data gathering processes and incomplete understanding of data.**

Another compliance requirement where capturing the location and usage of user personal data becomes key is **Data subject access requests (DSARs).** DSARs occur when users request the data that an organization has captured about them. To complete a DSAR request, organizations first need to understand which applications have what data regarding the requestee and in which location, which in certain cases is a manual process. Then the information is collected from all different locations and combined into a single response. The users also have the right to request the deletion and rectification of data. As such, organizations face challenges in **deleting data and verifying the deletion from all downstream systems.**

Data discovery and tagging

Many customers' personal information is discovered and collected from all around the world in local systems and transferred to other countries for storage and processing. The huge amount of data gathered is often raw in nature – it needs analysis and transformation to be valuable. To understand the data and manage access efficiently, security teams **discover it, scan it and tag it**. Without visibility into the source of data and alignment with the business, **there can be delays or worse, inaccuracies, in the tagging process**. An alternative option is to have data centers in each operating country

(or region) and conduct all stages separately for each data center, but this is **time-consuming and costly** for a global organization.

After the discovery of data, the data can be tagged based on data types and its origin. An organization has different types of data that includes, but is not limited to, material nonpublic information (MNPI), personal health information (PHI), personally identifiable information (PII), etc. There is a **risk of not identifying accurate origins and tagging certain types of data.** As management of access has dependency on data discovery and risk is compounded by probability of incidents and its consequences, the impact will be bigger.

Organizational risk management

One of the other challenges with cross-border is **how organizations approach risk.** Risk is a key element and a bridge between business and technology. When it comes to cross-border both regional and local risk should be taken into consideration. As regulations are advancing at high speed, the risk is always changing too and, therefore, should be closely monitored. Organizations must consider how multi-layered data protection strategies for data-at-rest, data-in-transit and data-in-use across cross-border (e.g., encryption, masking, tokenization, access control) can help mitigate these risks.

It is becoming more and more relevant to examine how organizations are securing their data and to examine their cyber coverage because a vast majority of privacy compromises and data breaches occur **due to lack of awareness, cyber capabilities and coverage.**

The risk further increases when the data is shared with or collected from a **third-party vendor**. Organizations faces challenges to apply and monitor the same level of cyber controls across third-party vendors and contractors.

Access management

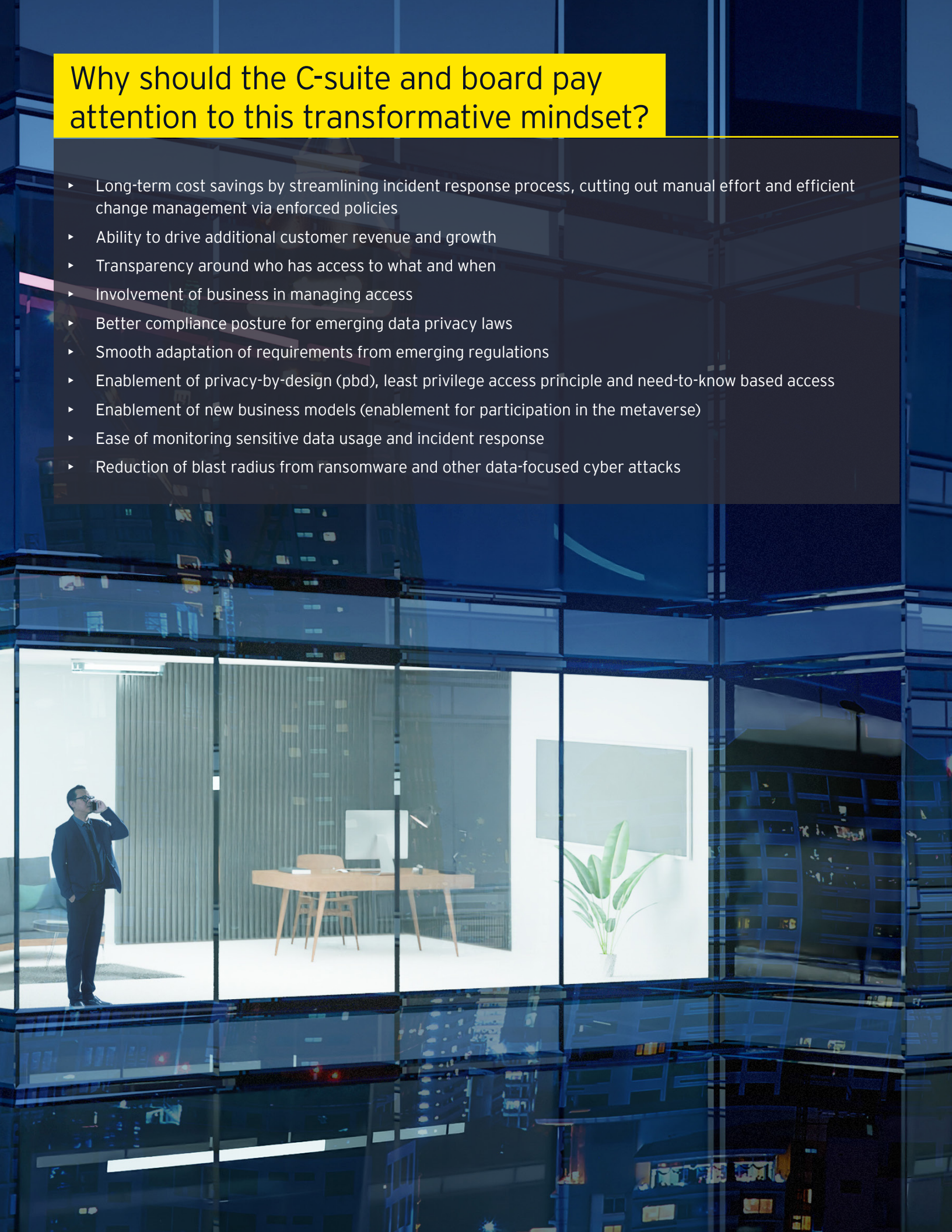
Many applications within organizations utilize regional data that is commingled and to operate normally, the users need access to the commingled data. With role-based access control still a common practice, **organizations create region-based roles to be in compliance which results in role explosion.**

The granularity at **column and row levels based on cross-border requirements** is challenging to achieve at the role-level and can expand existing role-based structures at a high rate.

With the responsibility of applying the principle of least privileged access along with data localization, the traditional methods of access management are increasing the cost and maintenance of expanding solutions. To mitigate risk, organizations must have **transformative mindset to cover Innovation at Scale, Humans at Center, and Technology at Speed.** Modern data protection solutions can complement access management strategies to enforce granular field-level policies to improve risk posture and regulatory compliance. Key-based encryption-in-use controls support the use of commingled data while at the same time keeping it segmented by applying different encryption keys to data from different regions. Such an approach also reduces the cost of least privilege access, since, by default, the data always retains encryption and is only decrypted for specific users based on policy.

Why should the C-suite and board pay attention to this transformative mindset?

- Long-term cost savings by streamlining incident response process, cutting out manual effort and efficient change management via enforced policies
- Ability to drive additional customer revenue and growth
- Transparency around who has access to what and when
- Involvement of business in managing access
- Better compliance posture for emerging data privacy laws
- Smooth adaptation of requirements from emerging regulations
- Enablement of privacy-by-design (pbd), least privilege access principle and need-to-know based access
- Enablement of new business models (enablement for participation in the metaverse)
- Ease of monitoring sensitive data usage and incident response
- Reduction of blast radius from ransomware and other data-focused cyber attacks



How does an organization transform their mindset to be more adaptable to ever-changing cross-border compliance changes?

To transform to be more adaptable to cross-border regulatory changes, organizations must look at a combination of transformations both on the core data protection side as well as on their approach to access control. Together these can provide a resilient and future-proof mechanism to address changes to data privacy regulations, threat environments, and internal security and privacy policies.

Organizations can mitigate the challenges of regionbased data access as well as data deletion requests by adopting a **modern data protection and access platform.** Core data protection should move from an individual data security controls application approach (encryption, tokenization, masking, etc.) to a systematic policy-driven data security platform (DSP) that **collapses controls into enforceable policies.** It can apply granular and variable security or privacy controls via policy based data security (PBDS). This can synchronize with an equally sophisticated policy based access control (PBAC) to produce a powerful global solution to the challenges.

The output of other security components can become an input for the PBAC model and help efficiently provision, remove, monitor, review, restrict and manage cross-border access. This collaboration between PBAC and other cyber controls will help organizations **apply and verify security policies consistently across the board.**

The policies are the natural language statements that will provide **transparency and visibility** to the business and leadership. Through policies, security controls can be understood in simple language; therefore increasing the involvement of **business** and their adaptation of ownership. Along with the involvement of business, the clear **definition and understanding of holistic user journey** that includes creation, consumption, processing and tracking data can help organizations manage and reduce data sprawl as much as allowed by data localization requirements.

The key security controls are spread across the following stages, which will help organizations adapt according to changing cross-border restrictions:

1. **Gather data from different countries.**
2. **Discover and tag the data.**
3. **Apply data protection.**
4. **Analyze access and control.**
5. **Monitor and enhance using other cyber controls.**

Gather data from different countries

- Gathering data from different countries into one single repository creates regulatory issues leading to the creation of multiple data centers, which is costly.
- Inability to discover new applications and repositories for data gathering is commonly observed.
- Organizations can utilize the **orchestration and innovative ways to view data** from multiple countries without changing the location of data storage where it is administered.
- Orchestration layer can lead **to coexistence of conditional access to the legacy and new systems to get the data,** where the conditions can be based on policies.
- Utilization of orchestration will allow IT to **adapt to changing business needs** without disrupting business itself. It also allows for the central automation of tasks and monitoring over different applications and repositories.

Discover and tag data

- Organizations face challenges in identifying the underlining location of the data. Sometimes the application or data owners are unaware of the geolocation. In such cases, organizations must implement creative ways to **identify geolocation automatically** and move away from dependency on applications or data owners' knowledge.
- Additionally, business must define and operationalize the standards for proper **creation, consumption and processing of data** which will reduce the complexity of discovery stage that comes as results of data sprawling.
- The **benefits of accurately discovered data** will be:
  - Sorted and well-understood data with a known location
  - Timely and automated identification of new apps and repositories from various locations
  - Reducing third-party risk, by identifying the location of their data

Apply data protection

- Application of encryption, tokenization, format-preserving encryption, masking or redaction to preserve downstream system functionality without any data exposure becomes key when data **is not only at-rest but also in-transit and in-use between different countries.**
- **Ability to apply granular protection based on region,** user-specific or regulation-specific policies and protect sensitive data as it flows across the organization will lead organizations to regional compliance.
- To meet the data protection regulations, organizations establish multiple point solutions to apply different data security controls that are inconvenient and costly. **Single data security policy source and enforcement** across all types of encryptions, tokenization, masking, etc., that can be used will **benefit** in the following ways:
  - Ease of data deletion
  - Ease of audit and forensics
  - Evidence of strong data security for regulators (National Institute of Standards and Technology, NIST, certificates)
  - Changes in business need will only require the change and enforcement of new policy

Analyze access and control

- It is commonly observed that there is a lack of clarity on which country can have access to **masked vs. unmasked data from which regions.** The utilization of masking rules from data protection and clear understanding of regionalization regulations from legal will result in application of the right level of access control.
- Creation of roles and resources based on countries, data masking, departments, lines of business, etc., has led to role explosion. **The policies based on regions and countries can be more efficient.** Any changes to the regulations can be applied by making updates to the policies rather than the creation of more roles.
- The biggest challenge is to **apply the same regional restrictions to the third party.** Capturing of contractor's accurate location during onboarding and an appropriate offboarding process will help organizations apply the same access policies to their third-party access. This will restrict contractors the same access to information from the countries that should be prohibited and beyond their contract period.
- **Business defines the needs.** It becomes a gap if businesses don't have visibility to access management. If businesses start defining and providing visibility to their policies, then organizations can avoid the time-consuming back-and-forth conversations between the business and IT to understand, define, review, and certify access.

Monitor and enhance using other cyber controls

- Lack of collaboration between access and other cyber areas is commonly observed. Therefore, to fulfil **DSAR deletion requests,** manual efforts are conducted to remove access from downstream system.

  The **policies** used to manage access are **not in alignment** with policies across cyber, for example, within data privacy and protection, insider risk, anti-money laundering (AML), governance, risk, and compliance (GRC), etc.
- Review of identities having access to high value assets is the key for **Insider Risk assessment** which is an isolated activity for most of the organizations.
- It is important for DPOs to understand **which access was removed to what entity and when.** To get such reports on a daily or weekly basis, DPOs follow a lengthy procedure or depend on an access team to produce it, which causes delays.
- Lack of a risk-based approach and varying AML requirements based on countries can lead to inconsistent implementation of **AML.**
- Lack of basic visibility to understand **whether data being passed to third parties** is aligned with Data Protection Impact Assessment (DPIA) or not.
- Lack of automated processes to **identify when a new unknown third-party is receiving data** but is not signed up with procurement systems or DPIAs.
- Many of these challenges can be resolved by efficiently **collaborating** with other cyber areas. **Monitoring outputs** from access management, discovery, and data protection can **enhance** cyber areas like insider risk, AML, data privacy, etc., and vice versa.

Conclusion

To apply ever-changing cross-border regulations consistently from an end-to-end cyber perspective, there is a need to transform from siloed cybersecurity strategies to a collaborative one.

In this era, gaining understanding on the location data and users has become critical. Along with this, the organizations can think through all the elements where they can successfully collaborate with or provide benefit to other cyber areas. This collaboration will help reduce repetitive and manual efforts. Eventually, automation can be established to utilize the knowledge of other cyber areas for improving data protection and access policies. Additionally, the knowledge and reach of access management to downstream systems or applications can be utilized by others within a cyber pillar. Such end-to-end collaboration and automation based on enforceable policies (even if they vary by region), will help organizations to quickly adapt to frequently changing regulations.

Authors and contributors

Varun Sharma
Principal
Technology Consulting,
Cybersecurity
Ernst & Young LLP
varun.sharma@ey.com

Sam H Tang
Managing Director
Technology Consulting,
Cybersecurity, Digital IAM
Ernst & Young LLP
sam.tang@ey.com

Angela Saverice-Rohan
Principal
Technology Consulting,
Cybersecurity, Privacy
Ernst & Young LLP
angela.savericerohan@ey.com

Kyle Harvey
Principal
Technology Consulting,
Cybersecurity
Ernst & Young LLP
kyle.harvey@ey.com

Jimmy Jin
Principal
Technology Consulting,
Cybersecurity
Ernst & Young LLP
jimmy.jin@ey.com

Nikolaus Ziegler
Managing Director
Technology Consulting,
Cybersecurity, Digital IAM
Ernst & Young LLP
nikolaus.ziegler@ey.com

Surbhi Tugnawat
Managing Director
Technology Consulting,
Cybersecurity, Digital IAM
Ernst & Young LLP
surbhi.tugnawat@ey.com

Kevin J Runyan
Senior Manager
Technology Consulting,
Cybersecurity, Digital IAM
Ernst & Young LLP
kevin.runyan@ey.com

Pankhuri Dawar
Manager
Technology Consulting,
Cybersecurity, Digital IAM
Ernst & Young LLP
pankhuri.goyal@ey.com

Austin E Brady
Manager
Technology Consulting,
Cybersecurity, Data Protection
and Privacy Consultant
Ernst & Young LLP
austin.e.brady@ey.com

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 003687-23Gbl
ED None

ey.com