Deloitte.

Cyber Strategy – The way forward

Deloitte Caribbean and Bermuda
October 1, 2020

Our Presenters

Cyber Strategy – The way forward

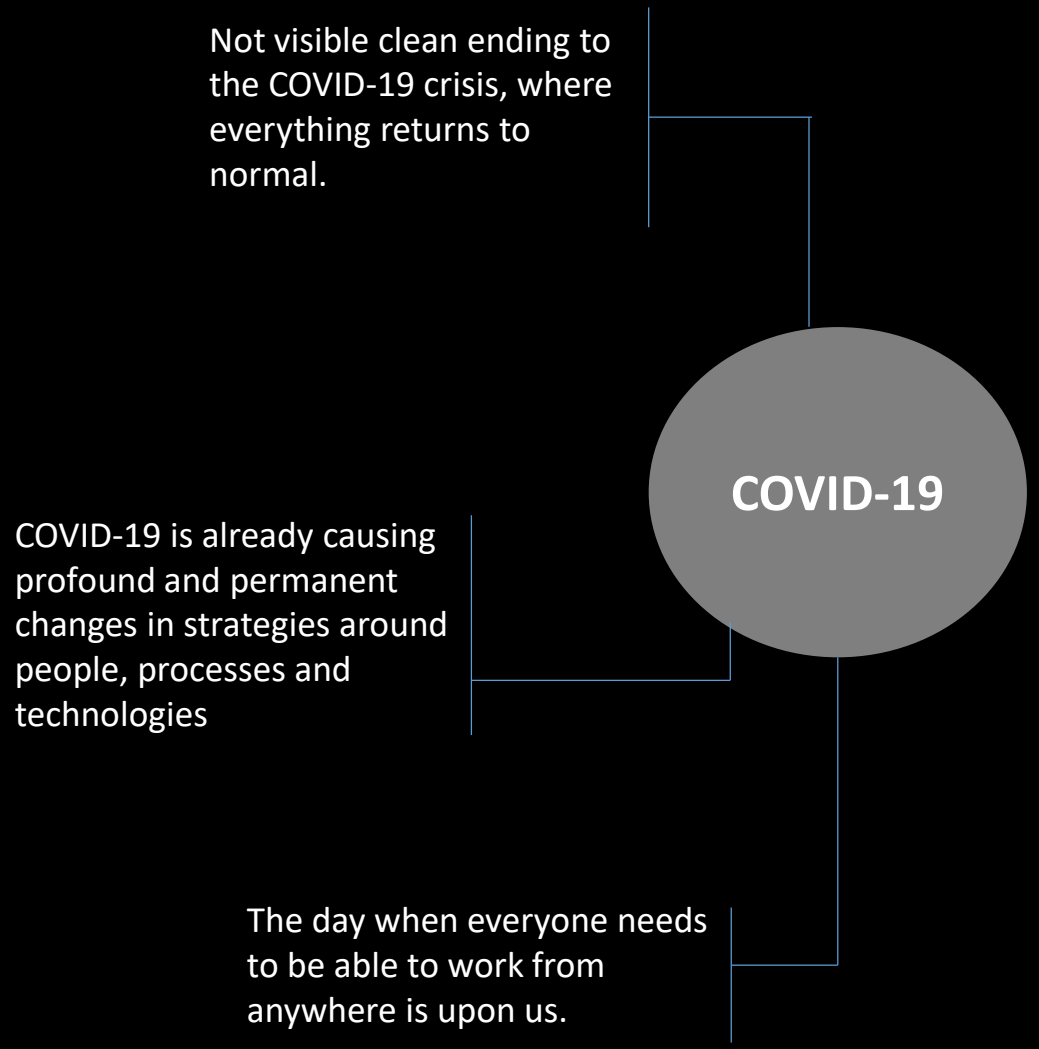
Cyber Fraud	Cyber Fraud	Cloud & Data	Privacy & Legislation	Privacy & Legislation	
Brett Henshilwood **Partner** **Bemuda**	Ramiro Basurte **Partner** **Argentina**	Wayne Green **Director** **Cayman Islands**	Rosena Duncanson **Senior Manager** **The Bahamas**	Dwight Robinson **Manager** **Barbados**	Q&A

Cyber Fraud

Dealing with risks, controls and mitigating actions for cyber crime and fraud

Brett Henshilwood: Partner – Bermuda
Ramiro Basurte: Partner – Argentina

COVID-19: Cyber Considerations



Prior to the COVID-19 outbreak **27% of users** globally worked remotely on the average weekday. As of March 31, 2020 this had risen to **more than 60%**

Between March 13-16, 2020 there were over **400k incidents** of spam emails pertaining to Covid-19

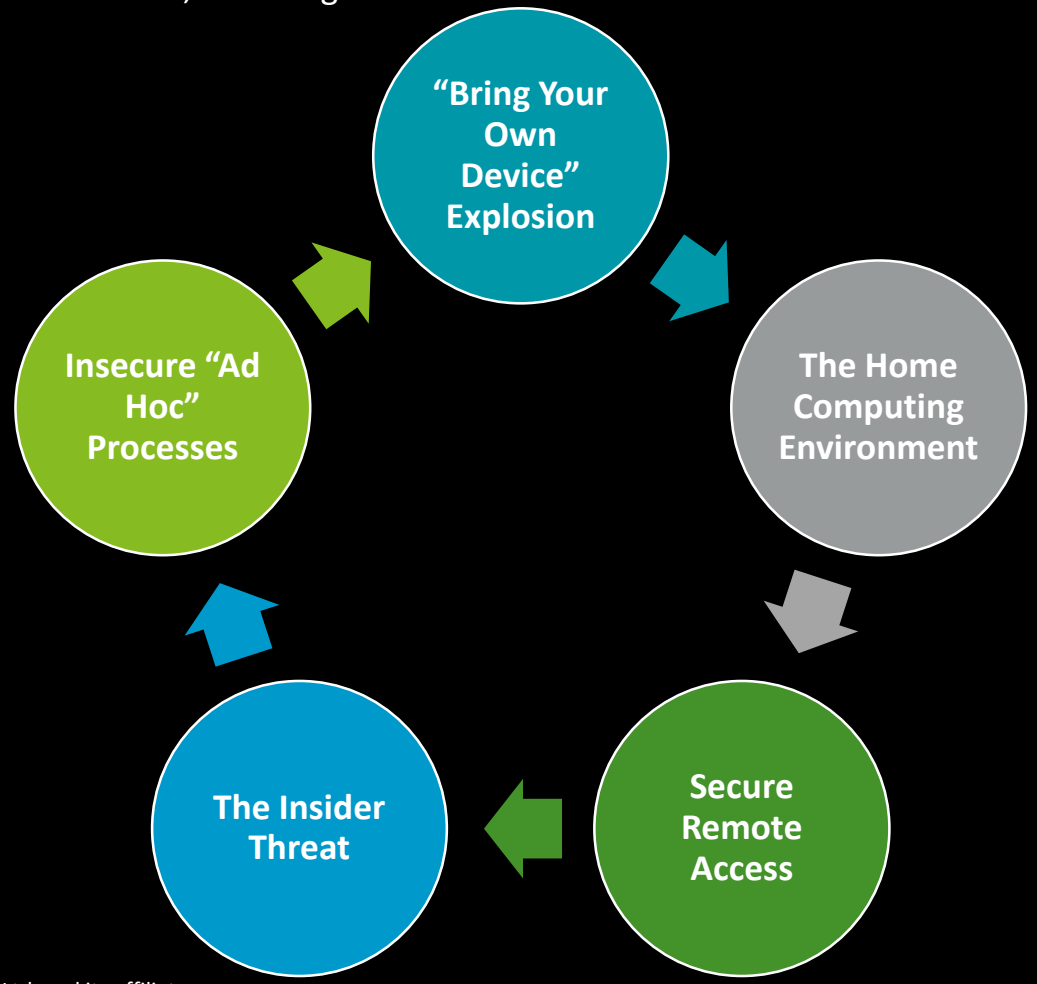
Without IT's knowledge **1,000+ insecure personal devices** connect to enterprise networks every day in 30% of UK, US and German companies.

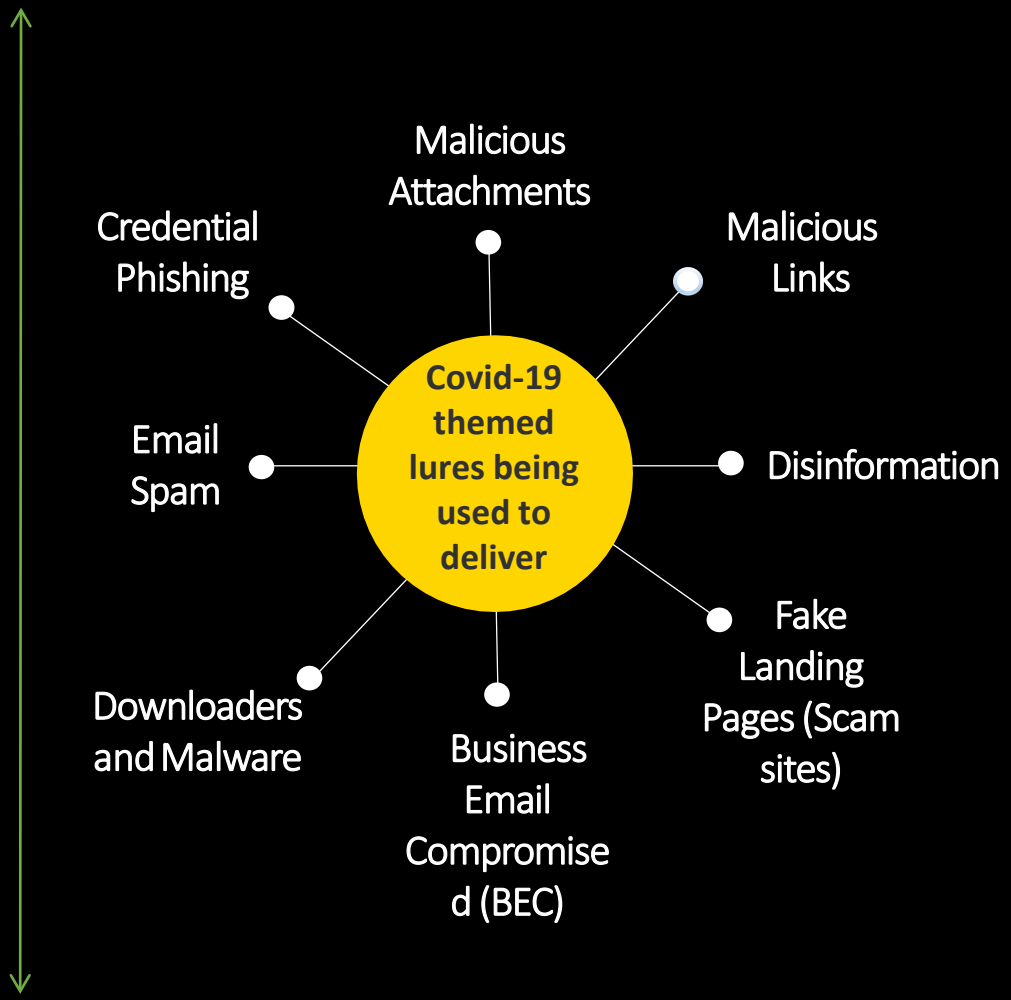
During the initial 'respond' phase technology decisions were largely made with an **operational, rather than a security** focus.

COVID-19: The Cyber threat landscape

The Next Normal

Almost overnight, enterprises worldwide found themselves in shut-down situations where workers had to shelter and work from home. This has created cybersecurity stressors across multiple dimensions, including:

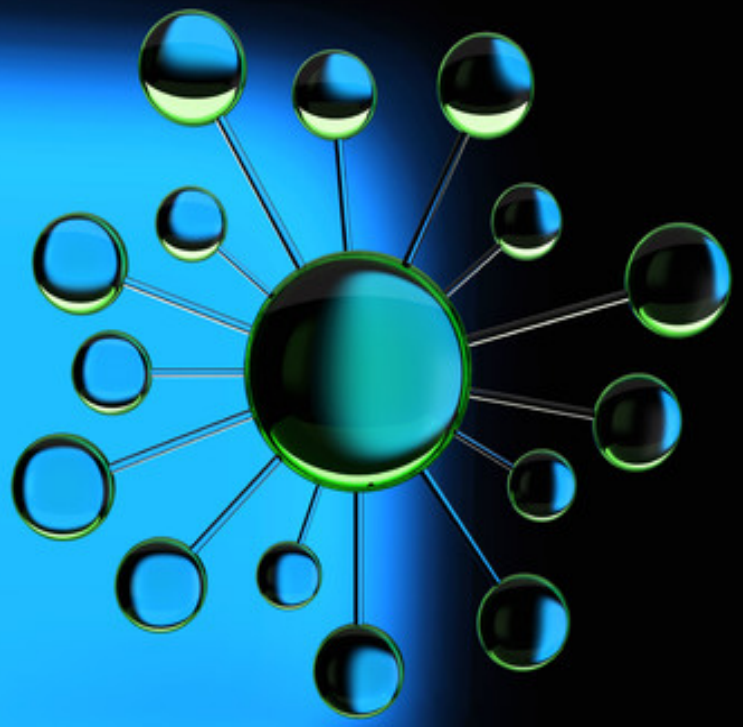




Phishing and other cyber threats

Attacking the people

Along with all problems created by the COVID-19 pandemic, attackers took advantage of this situation and the general concern by the people to target specific phishing attacks and fake corporate identities in order to gather intelligence and specific personal information as a way to carry out bigger and more complex attacks.



Directed Phishing attacks

Targeted phishing attacks using COVID-19 raised above all other attack techniques, aiming at banking clients, companies' end users and similar people in order to get specific information using "COVID-19 awareness" and similar topics.

Internal Phishing attacks

Similar phishing attacks were detected aiming at key personnel within important companies, aiming at getting user credentials, remote connections passwords and similar information, usually copying internal e-mail templates and wording, aiming at the regular end user.

Fake Corporate Identity

Mostly by using social networks as a means of approaching people, attackers faked corporate sites and social media accounts to get to clients, end users and potential prospects so they can, once again, gather all necessary information in order to launch more complex attacks.

Some companies shut down all their social media accounts informing their clients about the situation as a sudden measure to prevent information loss.

Collaboration tools – Controls and security considerations

Prevent camera and Screen-share hijacking

- Collaboration technologies should support private, password-protected collaboration environments/ zones
- In instances where this is not enforced, unauthorized users have “dropped” into meetings and taken control of the screen-sharing function to display illicit content and even gained visibility through a user’s video camera

Security needs Protect data and privacy

- Data collected from collaboration tools and platforms should not be shared/disclosed to third parties without prior consent
- Certain information/access should be prohibited, such as encryption key sharing, in foreign operating environments

Provide Robust content security

- Comprehensive support for end-to-end (E2E) encryption is critical to safeguard confidential content
- Some platforms and tools may support rigorous encryption standards, but may have exceptions for encryption support that leaves organizations vulnerable without the proper controls in place

Mitigation activities to consider

Do today

- Enforce auto-generated password use for meeting access
- Enable meeting waiting rooms and lock meetings once they have begun
- Disable custom meeting IDs and passwords
- Disable the ability to integrate with third-parties and social networks
- Request (from platform provider) that meeting codes be expanded to at least nine digits

Do this week

- Integrate collaboration technologies with Cloud Access Security Broker (CASB) solution to monitor for data exfiltration
- Maintain and enforce guidelines on platforms regarding meeting password access, meeting recording policies, and content transmission on the platform
- Push security awareness training for meeting hosts to reinforce secure collaboration practices, such as setting expiration dates for recorded meetings

Do next week

- Reissue meeting invitations as needed to include additional security layers
- Implement a web application firewall to detect and prevent application layer web-based attacks
- Enable Single-Sign-On to consistently enforce authentication rulesets
- Contact platform provider for additional information on specific organizational security requests and controls

Data protection – Actions to consider

Remote connection schemes

- End users access corporate resources through remote connection schemes, which are not always secure.
- Usage of home computers instead of certified corporate computers by end users present risks of software vulnerabilities to be exploited.

Volumetric controls

- Massive file copying activities are not always monitored and control, and in many cases, they represent an external attack extracting business information.
- User access to sensitive data should be restricted using the “less needed” principle and should include SoD (segregation of duties) activities and controls for critical business applications.

Reinforce policies implementation and data classification

- A data classification scheme should aid the different controls over data usage based on sensitivity, confidentiality and usage criteria.
- Data owners should be defined and informed.
- All policies and procedures related to data protection, classification and usage should be updated and properly communicated and published.

Mitigation activities to consider

Do today

Remind workers about their responsibilities to PI and PHI while working from home, including:

- Lock unattended devices
- Limit use of home printers
- Be mindful of confidential conversations

Execute awareness activities, such as informative e-mails, intranet messages, etc. to remind end users about the importance of keeping data secured.

Do this week

- Provide guidance on authorized devices, applications and transfer methods
- Reinforce secure storage and disposal practices (e.g., secure hard copies and shred printed documents)
- Have all remote connections scheme properly tested and reviewed by skilled vendors.
- Limit the use of home computers instead of corporate computers by end users.

Do next week

- Share policies, expectations, acceptable practices and available resources
- Review completion of on-boarding activities for contingent workers
- Reinforce insider trading policies
- Include ongoing data protection and non-disclosure responsibilities in third party and contingent worker departure materials.
- Implement volumetric controls over files servers and similar resources to control and monitor file copying and usage.

Thriving in the Future

This will drive renewed interest in technologies that enable secure remote access and productivity, including:

Virtual desktop infrastructure (**VDI**)

Cloud migration

Identity and access management (**IAM**)

The Future of People, Process and Technology

Enterprise performance is driven by people, process and technology. All three need to be addressed to effectively execute the digital transformation required to enable a world where remote workforces are the norm versus the exception.

People: People need to be "trusted but verified" to perform their duties in a suitable home environment without direct supervision, while also conforming to proper security hygiene and policy.

Process: Any process requiring physical interaction should be evaluated and, whenever possible, digitized to enable secure process execution in a remote-working environment.

Technology: Secure access, virtual desktops, remote device management and cloud-scale systems and applications will be critical to enabling the seamless transition from office to at-home environments.

Cloud & Data Storage

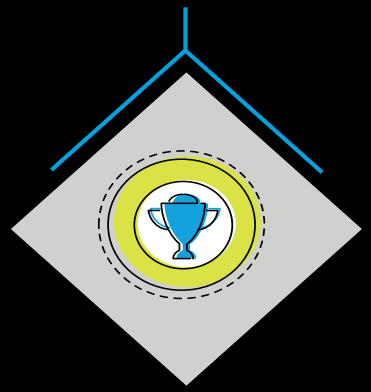
Considerations for governance and compliance, incident response and data storage

Wayne Green: Director – Cayman Islands

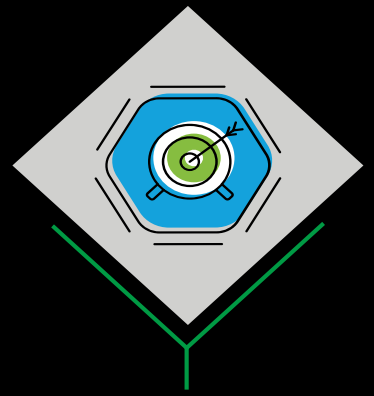
Cyber Considerations

Questions every executive should ask about their Cyber posture

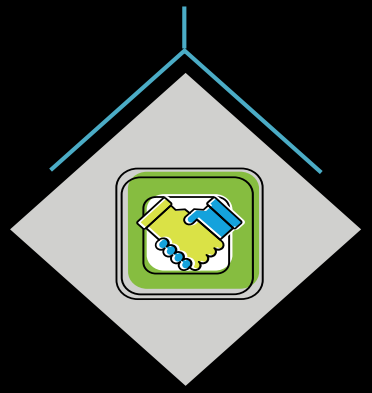
Have enterprise roles and responsibilities related to cybersecurity been clearly defined and communicated at every level of the organization up to the CEO and the board?



Do business leaders understand what the organization's most valuable assets are and the level of cyber risk they are accepting?

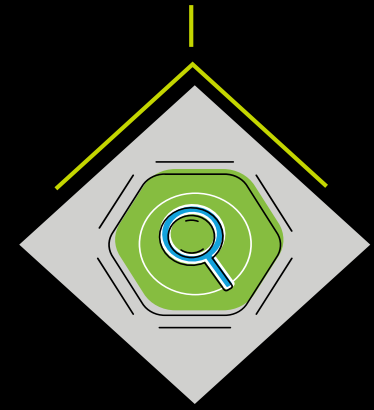


Are technology solutions designed, integrated, and operated with security and privacy in mind?



How should you reset your supply chain footprint to improve resiliency?

Does the business incentivize the adoption of cyber assessment and practices on the businesses and products in which it invests?



Are third-party (and beyond) risks managed with a cyber-risk lens in order to mitigate cyber impact directly or indirectly created from supply relationships?

Cloud Services Agenda

Governance and Compliance

Incident Response

Cloud Storage

Governance and Compliance

Risk and Concerns

Boards and executives recognize that cloud technology is now a strategic driver and enabler of business performance and share- holder returns.

Not having a secure cloud will diminish these value drivers result in regulatory fines, financial and reputational losses, and operational inefficiencies.

Challenges

Enterprises leverage multiple cloud delivery models (e.g., Infrastructure as a service “Iaas”). Identifying cloud assets and extending governance across multi-cloud and hybrid cloud eco-systems can be extremely challenging.

Governance and Compliance

Assess

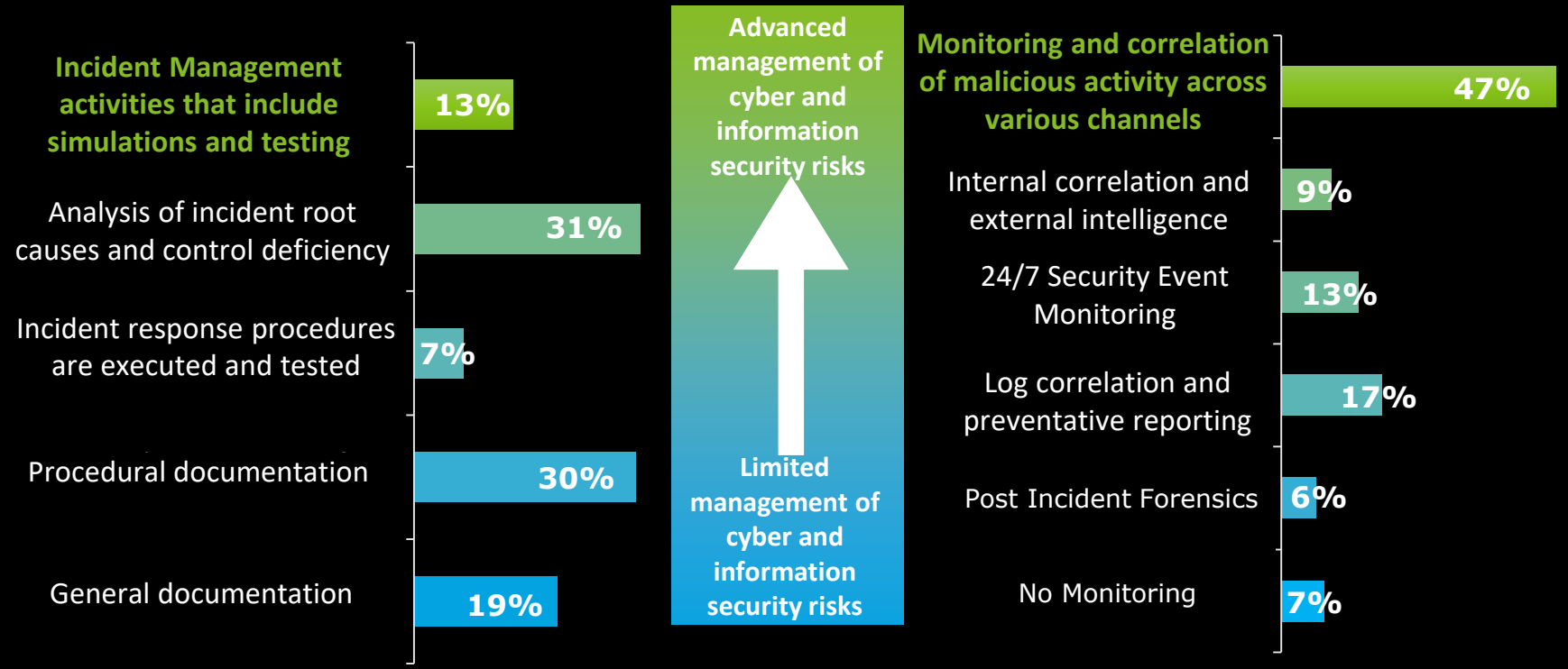
- Program initiation (cloud security program scope, charter etc.)
- Security and compliance planning
- Cloud security strategy (minimum secure cloud requirements and capabilities) and business case development
- Current state architecture review and technical configuration analysis/vulnerability identification
- Risk assessment and security requirements specification (integrated risk and requirements framework)
- Cloud security roadmap development

Design

- Cloud governance framework operationalized across the enterprise/control responsibilities
- Cloud security use case development
- Repeatable cloud security reference architecture patterns/designs
- Security technology and services (native, third-party) evaluation and selection
- Architecture, process, and technology integration design
- Implementation plan development
- Configuration management plan development

Deloitte Survey 2019

Cyber Incident Management



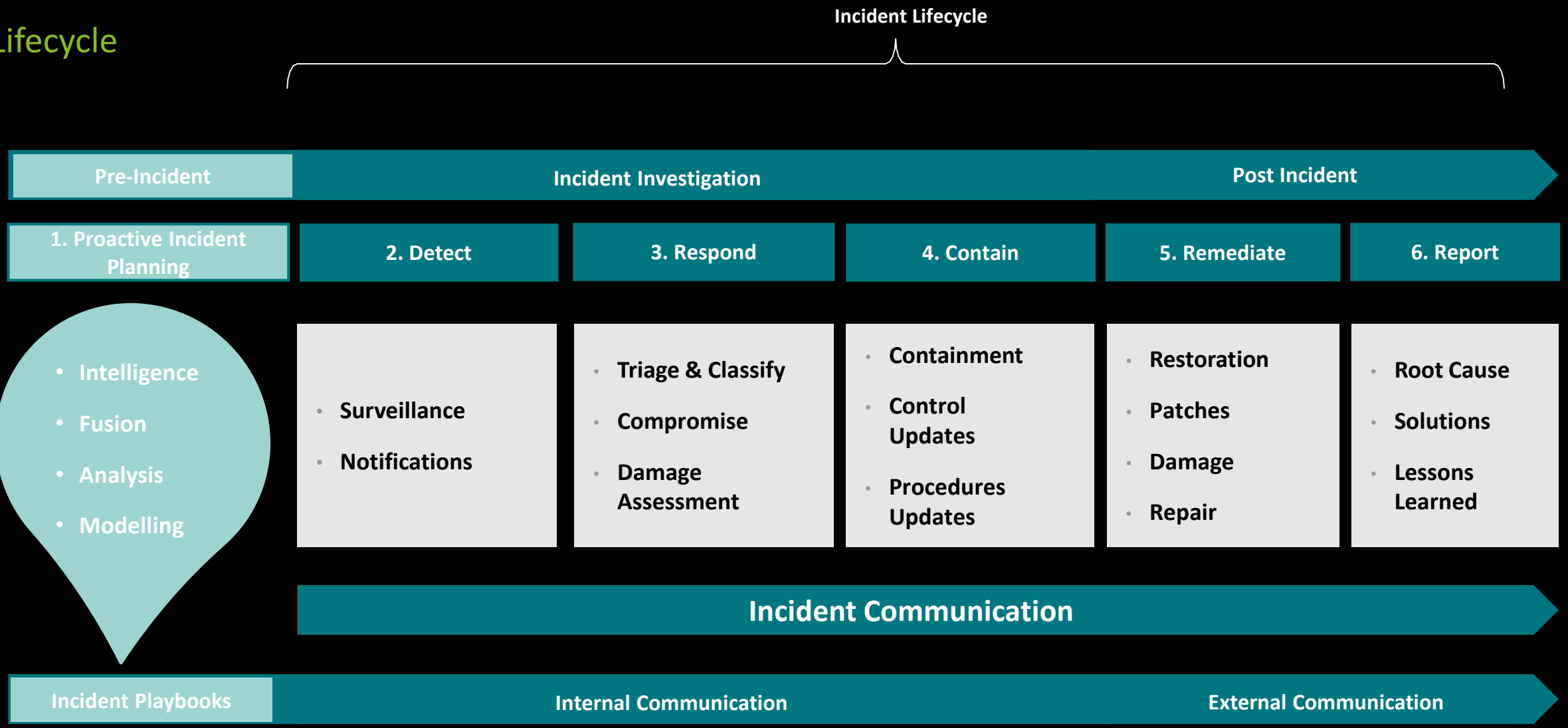
D

To be prepared to prevent and respond to cyber security incidents an organization should prioritize this as one of their strategic objectives.

Having a robust process, documentation, and testing continues to be a challenge for organizations.

Cyber Incident Response

Lifecycle



Data Storage Considerations

Cloud Environment

- Data privacy laws or local legislation
- Connectivity, application delivery (i.e. user interface or client delivery)
- Encryption
- Monitor the costs
- Backup

Privacy & Legislation

Leading Practices: Privacy & Cyber Legislation in the Caribbean and International markets

Rosena Duncanson: Senior Manager – The Bahamas
Dwight Robinson: Manager - Barbados

Why Privacy is Important

January 28th is **Data Privacy Day**, a day dedicated internationally to creating awareness of the importance of privacy and protecting personal information.

Data Protection Day commemorates January 28th, 1981, and the signing of Convention 108, an international legally binding data protection agreement on data protection.

Many of the data privacy regulations globally are based on the **OECD** Guidelines on the Protection of Privacy and Transborder Flows of Personal Data created in 1980.

Below are it's guiding principles:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability

Data Privacy Regulations in the Caribbean

Privacy Regulation Status Update

Country	Privacy Act	Enforcement Status
Antigua	Data Protection Act, 2013	Enacted by Parliament in October 2013
Barbados	Data Privacy Act, 2019	Passed in the Senate July 2019
Bahamas	Data Protection (Privacy of Personal Information) Act, 2003	**Effective from April 2nd, 2007**
Bermuda	Personal Info. Protection Act 2016	Privacy Commissioner appointed January 2020, Royal Assent in July 2016
Cayman Islands	Data Protection Law, 2017	**Effective from September 30th, 2019**
St. Kitts & Nevis	Data Protection Bill, 2018	Passed May 2018
Trinidad & Tobago	Data Protection Act, 2011	Limited sections enforced on January 6th, 2012

Business Impact Overview

Businesses are responsible for their roles (or outsourced roles) as a data controller

- Ensuring that the **Personal Data Processing Principles** are followed.
- **Responding to data subjects**' requests for information in a timely manner without delay.
- Overseeing that the processing activities carried out by a data processor are done in accordance with **technical and organisational security requirements**.
- Explicitly communicating to the data subject any **intent to transfer personal data** to another country or international organisation.
- Notifying the data subject should personal data be processed **beyond the purpose for which the data was collected**.
- Being responsible for ensuring the **consent of a data subject when data is collected** from someone other than the data subject.
- Ensuring that **appropriate security and risk measures** are in place to secure data including pseudonymisation and encryption.
- Ensuring the **confidentiality, integrity, availability** and **resilience** of processing systems in addition to periodic testing of the effectiveness of technical and organizational security measures.
- **Performing reviews** to ensure that processing is performed in accordance with the regulations and that at least risks associated with processing are addressed.
- Consulting with the Data Commissioner about **Privacy Impact Assessments** which indicate a High Risk level.

Data Controller

The Data Controller is a registered business appointed individual or representative who bears the responsibility for implementing the requirements of the Act including complying with the data principles of protecting personal data and abiding by the rights of data subjects.

The Data Controller is also responsible for ensuring that Data Processors who come in contact with personal information abide by the statutes of the Act by extension.

Business Impact Overview

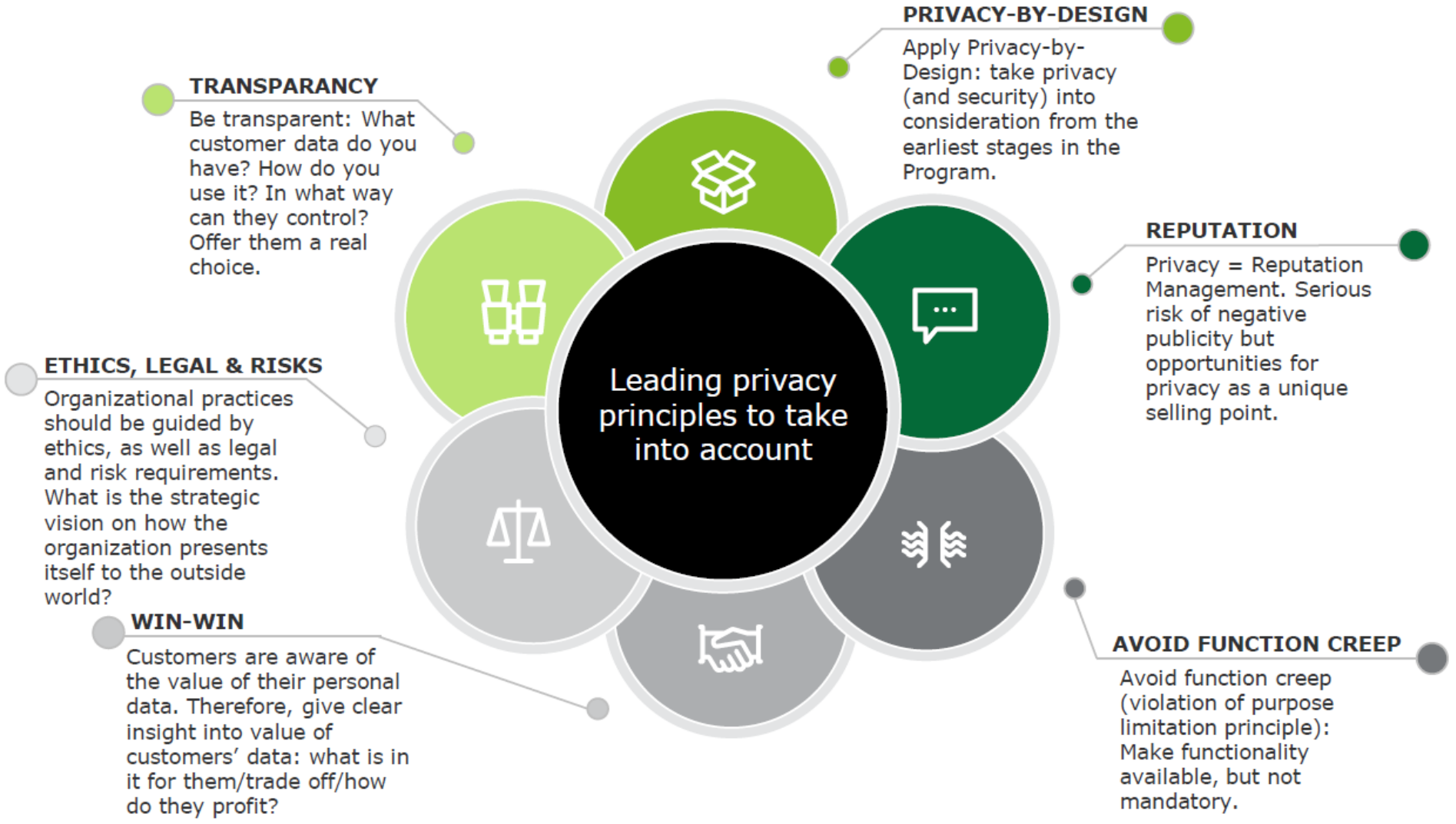
Privacy regulations have an impact throughout any organization which processes personal data. The table below shows how privacy related responsibilities are ideally supported.

Domain	Legal	IT/InfoSec	Compliance	Procurement	Business	HR
Data Breach Notification						
Data Security						
Data Subject Rights						
Organization & Accountability						
Privacy by Design/Default						
Privacy Impact Assessments (PIAs)						
3rd Party Disclosures						
Information Lifecycle Management						
International Data Transfers						
Monitoring & Enforcement						

● Heavy involvement required ○ No involvement required

Deloitte’s view of Privacy

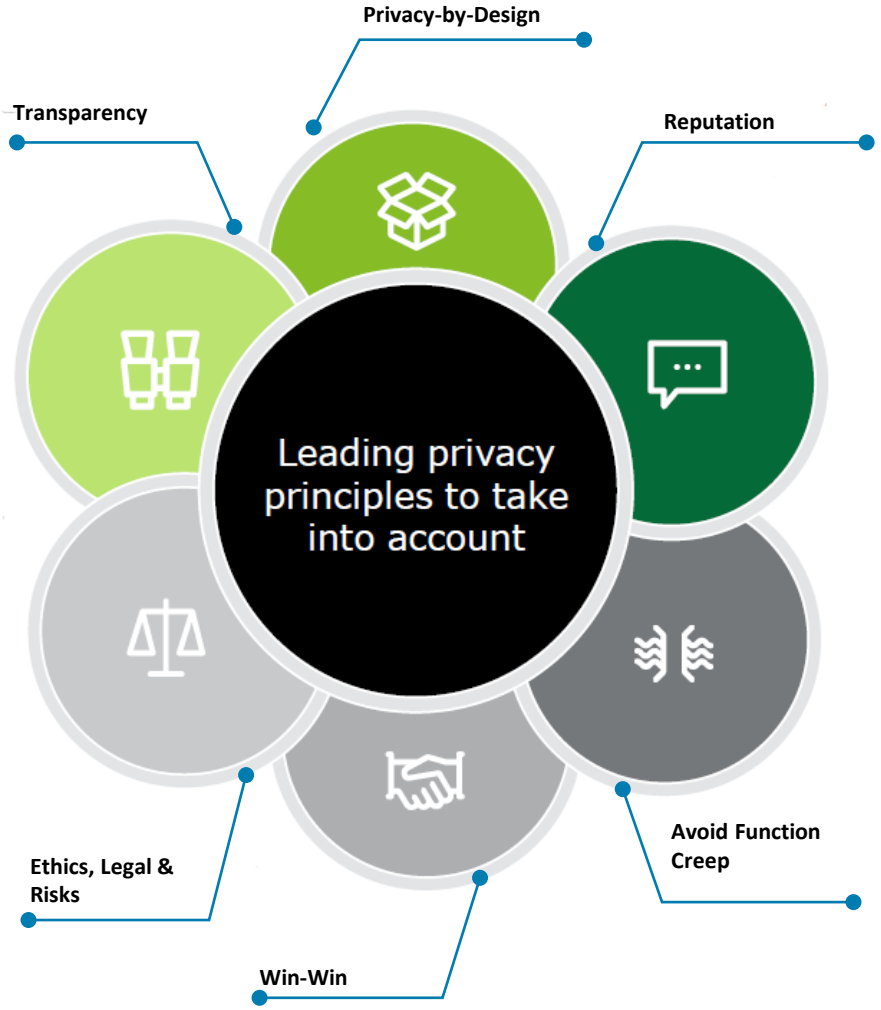
The diagram below shows Deloitte’s view of Privacy and how it should be considered for its impact on businesses and individuals.



Foundational Principles of Privacy by Design

Privacy by Design is an important part of the privacy structure. Under Privacy by Design, privacy is seamlessly integrated into every business process and the development of new systems, not bolted on at the end. Some of the key tenants of Privacy by Design include:

- **Proactive not Reactive; Preventative not Remedial**
- **Privacy as the Default Setting**
- **Full Functionality – Positive-Sum, not Zero-Sum**
- **Visibility and Transparency – Keep it Open**
- **Respect for User Privacy – Keep it User-Centric**



Data Privacy Enforcement

Privacy standards require a change in business culture towards how private data is handled. Policies need to go beyond establishing a minimum regulatory compliance approach.

Businesses need:

- GDPR , data privacy knowledge & readiness assessments
- Accurate Data inventory/ mapping
- Application of technology tools & accelerators for efficient risk & regulatory management
- A focus on key workstreams to enforce the necessary processes to meet local and international Privacy law requirements

Deloitte has developed a framework around eight workstreams to enable effective enforcement & compliance

We have a regional & global privacy team and project management team that is unrivalled in terms of its combined size, knowledge, experience and capability

Prioritizing enabling technology for Privacy

In the next 6-8 weeks, technology requirements must be determined in order to support an effective transition to design and implementation.

Privacy Key Technology Capability	Prioritization		
	Do Now	*Do Next*	*Do Later*
Consent Management	X		
Portability			X
Erasure			X
Data Protection Impact Assessment	X		
Security (e.g) • Encryption / Tokenization / Pseudonymization • Data Leakage Prevention (DLP)	X		
Personal Information Processing Inventory	X		
Third Party Privacy Management			X
Privacy Incident Management			X
Privacy Complaints Management and Individual Rights		X	
Cookie Management	X		

Things to Consider

- Where are we building the Tech framework for Privacy?
- Are there any existing systems that can enable Privacy requirements?
- If systems are not available, has the solution selection process started for any of the requirements?
- What is the timeframe for the typical solution selection cycle?
- Do we need to prioritize the technology solutions for each of the Privacy requirements?
- Delays in selecting systems will impact the implementation plan

Privacy Transformation Program: Methodology

Realization of every work product in the focus areas allows a fixed approach

Focus Area 0 : Governance

Structuring the privacy organization as well a the roles, responsibilities and positions of key players.

Focus area 1: Guidance and instruction

Providing practical guidelines and clear working instructions to achieve privacy compliance

Focus area 2: Awareness & Communications

Embedding privacy awareness in the organization and design internal and external communication plan.

Focus area 3: Privacy operations

Building DPIA methodology and Privacy by Design processes to incorporate privacy in daily Programs.

Focus area 4: Processing inventory

Setting up an processing inventory enabling systems to demonstrate control over processing activities

Q&A

Brett Henshilwood
Partner, Deloitte Bermuda

Ramiro Basurte
Partner, Deloitte Argentina

Wayne Green
Director, Deloitte Cayman Islands

Rosena Duncanson
Senior Manager, Deloitte Bahamas

Dwight Robinson
Manager, Deloitte Barbados

Deloitte.

Deloitte Caribbean and Bermuda