THE INTRINSIC VALUE OF ENSURING DATA PRIVACY

ROBERT VAN VIANEN
PARTNER,
CYBERSECURITY & PRIVACY ADVISORY
BDO NETHERLANDS

KAREN SCHULER
PARTNER
DATA & INFORMATION GOVERNANCE LEADER
BDO USA

According to the 500 global business leaders surveyed in the BDO Global Risk Landscape report 2017, disruptive technologies, reputational risk and cybersecurity are the challenges most likely to test businesses over the next ten years.

Additionally, BDO USA's 2017 Cyber Governance Survey found that 79% of public company boards are more involved with cybersecurity today than they were 12 months ago, with 78% having increased company investments within the past year to better defend against cyberattacks.

In this paper BDO seeks to demonstrate how building a mature information security and data privacy programme can enhance the professionalism of a company's employees and reinforce an organisation's public reputation.

It provides insight on the intrinsic value and sometimes more difficult to quantify hidden benefits that organisations can achieve through meeting and exceeding their data protection obligations.

THE IMPORTANCE OF DATA PRIVACY IN PROTECTING AGAINST CYBERCRIME

The GDPR comes into effect on 25/5/18. Compliance with the new regulations will require good data hygiene in the form of purposeful collection, protection of sensitive information and adherence to retention programmes that remove expired information. In assuring each of these, companies can expect to achieve more than mere compliance and penalty avoidance, but also to lower the cost of infrastructure and operations and to help employees and managers gain quick access to good information to support business decisions.

In recent years there has been a huge shift in the importance placed on data privacy. Cybersecurity is no longer just an IT issue. It has captured the attention of boards and senior executives. According to BDO USA's 2017 Cyber Governance Survey, this is the fourth consecutive year that board members have reported increases in both the time and expenditure devoted to cybersecurity, of which information governance and data privacy is a direct component. 78% of company directors say they have increased company investments during the past year to defend against cyberattacks, with an average budget expansion of 19%.

PUBLIC COMPANY BOARDS MAINTAIN POSITIVE TRENDS ON CYBERSECURITY

	2014	2015	2016	2017
Increased Board Involvement	59%	69%	74%	79%
Increased Cybersecurity Investments	55%	70%	80%	78%
Incident Response Plan in Place	NA	45%	63%	61%
Cyber Breach in Past Two Years	NA	22%	22%	18%

Reference: 2017 BDO Cyber Governance Survey

As a business owner or company executive, are you considering:

- The benefits and intrinsic value of investing in data security and data privacy, beyond merely ensuring legal compliance?
- How tackling data security and data privacy can benefit your organisation?
- How you can lead and contribute in the right way to realising these benefits?

BDO CAN HELP

IMPLICATIONS OF GDPR FOR BUSINESSES IN 2018

Art. 32 'security requirements' of the GDPR requires companies and organisations to become more structured and formal in how they protect personal information, including requirements for purposeful collection, transparency, data minimisation and support for data subject rights.

Key requirements of the GDPR include:

- Mandatory data inventory and record-keeping of all processing of European personal data
- Mandatory data-breach notification to regulators and individuals whose information is compromised
- The right to be forgotten, which allows individuals to request that their personal data be erased
- Routine privacy impact assessments (PIAs)
- Mandatory data protection officers (DPOs)

In order for employees to properly handle information on a day to day basis, the GDPR warrants a full awareness and training programme involving the privacy aspects of information. Is is best practice to combine data privacy and cyber security awareness and training programmes and employees will be required to attend such training programmes and to be able to access the management oversight, tools and audits for effectiveness in order to verify that programmes are working as designed.

The GDPR contains fixed conditions for companies to pass on the requirements for data privacy in formal legal agreements. It is worth noting that organisations are increasingly being held accountable by their corporate clients who are implementing third-party risk management programmes.

The Talk Talk cyber breach (UK, October 2015), affected nearly 160,000 customers and resulted in a record fine of £400,000. Under GDPR, if that attack occurred again, the potential penalty could be as high as €17 million.

THE HIDDEN VALUE

HOW TO LEVERAGE GDPR TO YOUR ADVANTAGE

For many managers, the GDPR is just one of many new laws that have to be implemented within their organisation. The GDPR, however, should be seen as the starting point of a process in which you create a stronger foundation for your organisation's strategy. A solid information governance programme can bring real benefit in both new opportunities for revenue, as well as in cost reduction for data storage and reduced inefficiencies when employees are unable to locate or use outdated information, to inform decisions.

Working on data security in a systematic, professional manner means assessing risk and focusing efforts and investments on the areas where they are needed. Organisations that do this are able to streamline performance, reduce costs and reap hidden benefits in the following areas:

- **Risk Management & Corporate Accountability**
- **Data control operations**
- **Client, Supplier and Employee relations**

> "The added benefits of possessing a mature data privacy programme are scarcely considered and organisations are simply concentrating on compliance and avoiding fines. This creates a tick-box culture that does not inspire going beyond minimal requirements with respect to cybersecurity and data privacy."
>
> **ROBERT VAN VIANEN,**
> PARTNER, CYBERSECURITY & PRIVACY ADVISORY, BDO NETHERLANDS

At BDO, we deliver a range of information governance, data privacy and cybersecurity services. When it comes to GDPR, we use a three-phased approach. First, we evaluate the impact that GDPR will have on your organisation. We then assist you to implement the changes required to achieve compliance. Once compliant, we review your program on an annual basis in order to ensure continued compliance.

CHANGE MANAGEMENT
Provide skilled change management professionals to ensure the project is run in a structured manner, reporting regularly to company management, driving the project forward at a pace that fits company culture culture and meets the required deadlines.

GOVERNANCE FRAMEWORK DEFINITION
Put in place a relevant structure for GDPR to be implemented in a controlled and governed environment. This includes implementing an Information Governance Framework within the organisation.

EDUCATION & TRAINING
Provide company employees with an in-depth understanding of the key requirements of the new legislation and the impact on the organisation. Deliver workshops to collaboratively define an approach to ensure cultural change.

POLICIES & PROCEDURES
Review clients' existing policies & procedures to identify any gaps against the upcoming legislation. If required, a set of policies & procedures can be created for clients based on best practices.

Reference: BDO GDPR Services

RISK MANAGEMENT & CORPORATE ACCOUNTABILITY

STAY INFORMED, DEMONSTRATE ACCOUNTABILITY AND IMPROVE YOUR REPUTATION

Executives typically agree that data privacy and security are important, yet few of them have in-depth knowledge in this area to reassure clients, consumers and investors that their organisation has sufficient protective measures in place. According to BDO USA's 2017 Cyber Governance Survey, 23% of corporate directors do not know whether their organisation has a cyberbreach/incident response plan in place.

A formal programme with a third-party assessment and results reported to the board can help key stakeholders remain informed, reduce risk and support strategic and investment decisions. A well-informed executive board that has been regularly engaged in the organisation's cybersecurity dealings also significantly strengthens its defensive position in the event of a breach or complaint.

The 'accountability' principle under the GDPR requires organisations to create and maintain a record of processing activities so they are able to demonstrate compliance, as well as the factors used in the 'balancing' decisions on risk.

Those who are able to demonstrate 'accountability' and have met their legal obligations strengthen their position and reputation with supervisory authorities, clients, consumers and investors.

In recent years high-profile data breach events have left no doubt that even large, well-known companies are unable to guarantee the protection of the growing mountain of sensitive personal information. And the consequences of failures can be severe. For example, as a result of reputational damage and within one week of the breach disclosure, Equifax saw its shares drop 20% - an amount equivalent to roughly US$4 billion.

BDO USA's 2017 Board Survey found that 52% of organisations have processes in place to conduct regular cyber security risk assessments, but only 40% of organisations have a process in place to conduct third party/ vendor risk assessments. This means that many organisations do not have repeatable processes in place to consider and assess their cyber risk exposure and how these may impact the business.

DATA CONTROL OPERATIONS

CONTROLLING YOUR DATA AND ASSOCIATED COSTS

The GDPR requires 'data minimisation' in the form of collecting, using and retaining only what is necessary for the purposes of processing. Extraneous or expired information is not to be processed. This is in stark contrast with the 'gather it all and sort it out later' / 'keep everything indefinitely - just in case - because storage is cheap' philosophies that many businesses have accidentally adopted.

Over the years, we have found that while disk space is indeed cheap, storing and maintaining data is certainly not. The GDPR's push toward cleaning out the corporate closet can be used to eliminate unnecessary information and the associated storage costs.

The side benefit to this is that without the haystack of expired, extraneous information, managers and employees will be able to find the proverbial needle they need faster - and be less apt to use outdated, inaccurate information to support decisions. But perhaps most important is the benefit of improved corporate citizenship by reducing the risk of identity theft and financial fraud to the employees, prospective customers and clients whose information is entrusted to the data controller.

CLIENT, SUPPLIER AND EMPLOYEE RELATIONS

BUILDING TRUST

An organisation with a good data privacy and information security programme can demonstrate to its business partners, employees and clients that their data is in good hands. This makes the organisation a reliable and trusted partner with which to do business.

> "One thing that an information-secure organisation never does is hide behind a software supplier - or any vendor for that matter - that states it is 'GDPR-certified' or 'GDPR-ready'"
>
> **ROBERT VAN VIANEN,**
> PARTNER, CYBERSECURITY & PRIVACY ADVISORY
> BDO NETHERLANDS

GDPR requires contractual provisions that clearly state responsibilities, and this should be best practice even for entities not subject to GDPR. An overall third-party information risk management programme should be instituted to assess risk for any vendors with access to personal data, and to require specific protective controls that are relevant and proportionate to the risk.

> "A professional and responsible data security programme proves that your organisation takes protecting the privacy of its clients and employees seriously"
>
> **KAREN SCHULER,**
> PARTNER, DATA & INFORMATION GOVERNANCE LEADER
> BDO USA

By shouldering that responsibility, an organisation engaging with its suppliers to discuss proper data security can expect both structural improvement and a more mutually beneficial long-term relationship.

STRENGTHENING EMPLOYEE RELATIONS

Human behaviour is the number one cause of data incidents and data breaches. The introduction of the GDPR - aimed at instilling more control - creates an excellent opportunity to educate employees and raise awareness of data privacy and cyber best practices. The provision of security and privacy awareness training empowers employees, who represent the most important actors in your data protection programme.

- Data security involves holding people at all levels of the organisation accountable for their professionalism. This increases possibilities for new standards of effectiveness and efficiency
- A clear picture of the data flow provides insight into how matters can be improved and be made safer – as well as more efficient and less expensive
- It offers an opportunity to work on process optimisation
- It lays the foundations for identifying new growth opportunities, such as big data.

CONCLUSION

Ensuring a mature, professional data privacy programme is extremely important for every organisation. Regardless of the legislation, penalty clauses and all the threats that exist in this area, any and all organisations would benefit from investing in, and guaranteeing the protection and proper handling of data under their management. Information is often a corporation's most valuable asset. By developing the comprehensive governance, risk and compliance programs required by the GDPR, organisations lay a solid foundation for proper information governance and data privacy. Moreover, the extent to which an organisation is ready for impending technological developments could determine the future growth and success of that organisation in the coming decades.

> "Information is at the heart of every organisation, and ensuring the security of that information is crucial"

KAREN SCHULER,
PARTNER, DATA & INFORMATION GOVERNANCE LEADER
BDO USA

CALL IN THE EXPERTS

BDO's Global Cybersecurity practice is comprised of professionals from a diverse range of backgrounds, including experienced IT, operations, and data privacy consultants, as well as forensic technology, business advisory and accounting practitioners. We are structured to provide comprehensive, customised services for each client, focusing on your specific operating model, technical demands, regulatory environment and industry dynamics. Whether it's financial services, healthcare, retail, natural resources or any other industry – we understand your needs.

Our global footprint extends to every corner of the globe and so does cybercrime. Let us help your organisation, wherever you are, to mitigate the cyber risks you're facing.

ABOUT THE AUTHORS

Robert Van Vianen

Robert is a managing partner in the Cybersecurity & Privacy advisory practice within BDO Netherlands, whose main focus is on the Public Sector, including healthcare. Robert has more than 17 years' experience in the areas of cybersecurity, data privacy and risk management.

Karen Schuler

Karen Schuler has more than 25 years of experience managing global organisations that provide privacy, security, and e-discovery services. As a testifying expert and well-known presenter and author on high risk corporate issues impacting global organisations, she has held executive level positions for some of the largest service providers, is a former member of the United States Securities & Exchange Commission, and is BDO's Data & Information Governance Practice Leader.

ABOUT BDO'S GLOBAL CYBERSECURITY LEADERSHIP GROUP

Our corporate methodology incorporates several proprietary models for supporting organisations in developing and improving their cyber security posture. From establishing compliance and building a proactive approach through the ongoing development of capabilities, to effective security risk management, we work with our clients to quickly attain higher levels of maturity and resilience.

GLOBAL CYBERSECURITY LEADERSHIP GROUP

GREGORY A. GARRETT
HEAD OF INTERNATIONAL CYBERSECURITY

BDO USA
+1 703 770 1019
ggarrett@bdo.com

GRAHAM CROOCK
DIRECTOR, IT AUDIT, RISK & CYBER LABORATORY

BDO South Africa
+2782 606 7570 or +2782 465 4539
gcroock@bdo.co.za

SANDRA KONINGS
PARTNER, CYBERSECURITY

BDO Netherlands
+3165 150 8151
sandra.konings@bdo.nl

LEON FOUCHE
PARTNER AND NATIONAL CYBERSECURITY LEAD

BDO Australia
+6173 237 5688
leon.fouche@bdo.com.au

ANDREAS VOGT, PH.D.
DIRECTOR / HEAD OF SECTION, BDO SECURITY & EMERGENCY SERVICES

BDO Norway
+4748 171 714
andreas.vogt@bdo.no

JASON GOTTSCHALK
PARTNER, CYBERSECURITY PRACTICE LEADER

BDO UK
+4479 7659 7979
jason.gottschalk@bdo.co.uk

OPHIR ZILBIGER, CISSP, CRISC
PARTNER, HEAD OF SECOZ CYBERSECURITY CENTRE

BDO Israel
+9725 2675 5544
ophirz@bdo.co.il

FOR MORE ON BDO CYBERSECURITY, VISIT:
CYBERSECURITY.BDO.GLOBAL

FOR MORE INFORMATION:

CYBERSECURITY.BDO.GLOBAL

Twitter:
@BDOglobal

Email:
marketing@bdo.global

Editorial: BDO Global Office, Belgium

www.bdo.global

HB010212