How to overcome your data security compliance challenges

IT governance™

Protect • Comply • Thrive

As cyber attacks continue to dominate headlines and data breaches become more commonplace, it is clear that businesses are struggling to effectively manage increased cyber risks.

The growing threat of data breaches in the US

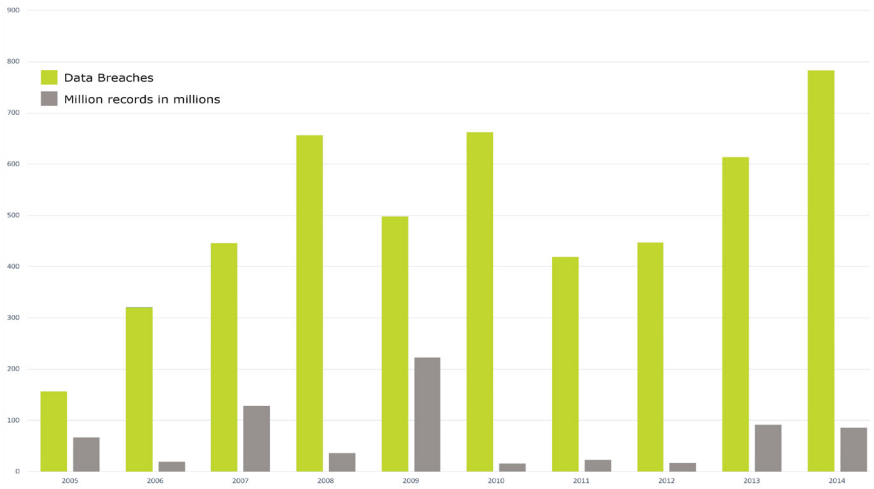
Between 2005 and 2015, the number of records breached by cybercriminals in the US increased dramatically, from 157 million to 781 million. In recent years, a number of high-profile companies and organizations have been victims of cybercrimes, including HP, Oracle, Verizon, the Democratic National Committee, and Yahoo! In 2017, the US has already seen its fair share of major cyber incidents involving Equifax, Deloitte, Merck and Virgin America. According to the latest Breach Level Index report, in the first half of 2017, there were 918 reported data breaches and nearly 1.9 billion compromised data records worldwide.

No level of security technology is going to fully protect your business from an attack

Cyber criminals act indiscriminately as they find new ways to exploit vulnerabilities in software, systems, networks, and even staff. Cyber attacks are ever-present, becoming more severe and causing lasting consequences. Affected firms can lose public trust, suffer falling share prices, and face sanctions for breaking the law.

"1.9 million compromised data records worldwide."

Annual number of data breaches and exposed records in the United States from 2005 to 2016 (in millions).



Confusion over the cybersecurity regulatory environment can cause missteps.

In the US and internationally, regulatory agencies are now demanding that organizations – large and small – take responsibility for securing sensitive data in their custody.

New and evolving federally mandated cybersecurity regulations are forcing organizations to implement policies and standards to secure their information systems while protecting personal data.
Some noted regulations worth mentioning are:

- 1999 Gramm-Leach-Bliley Act
- 1996 Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- New York's DFS Cybersecurity Regulation (23 NYCRR Part 500)
- EU General Data Protection Regulation (GDPR)

It is essential for every organization to protect data and information systems at a basic level. To learn more about Federal Cybersecurity and Privacy Laws, visit our web page directory >>

Even more regulatory pressure

President Trump's Executive Order 13800 is the new administration's attempt to strengthen digital security and infrastructure. EO 13800 calls for the national alignment of policies, standards, and guidelines. Issued on May 11, 2017, the implementation is still in the analysis and planning stages.

In the meantime, a number of states across the country are taking their own protective measures. For example, several have created regulations similar to the Notice of Security Breach Act passed by California in 2003, which requires organizations maintaining information about Californian residents to provide breach details whenever personal data is compromised.

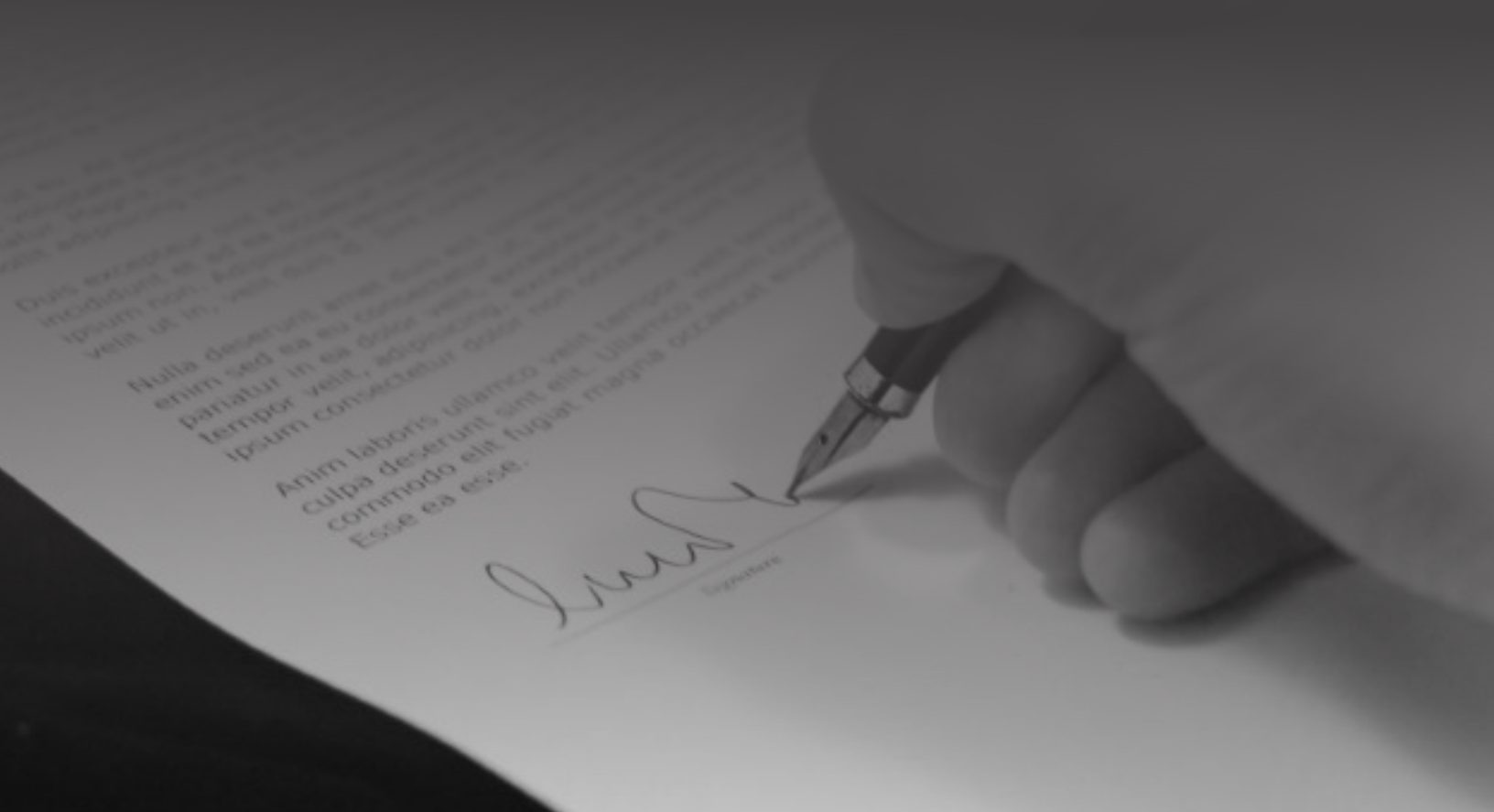
The New York State Department of Financial Services enacted the first-in-the-nation cybersecurity regulation, NYCRR 500 and established compliance on August 28, 2017. NYCRR 500 compels banking, insurance, and financial institutions to protect consumer data and information system infrastructure. At least a dozen other states are following suit by instilling broader cybersecurity measures.

Despite the tightening of cybersecurity legislation, what some business leaders still do not realize is that organizations have to comply with the law before they are breached – not only when the breach has already occurred. It is their legal responsibility to eliminate conditions that could lead to a potential breach and put plans in place to respond to any breach should one occur.

Cybersecurity is challenging with no unified law

With no unified law regulating cybersecurity, IT and security executives are hard pressed to cover all the different laws with one solution. For example, with the exception of HIPAA, no centralized US regulation defines how private, non-profit, or government entities should notify data subjects in the event of a breach. Rather, 48 states and four of the territories have their own, specific laws.

One of the most difficult aspects of IT security is understanding which federal laws apply to your organization, without even considering state and local legislation. CIOs, security officers, and those under their direction (including contractors) must navigate all the relevant acts, presidential executive orders, and guidelines, and possess the know-how to apply them in the most efficient, cost-effective way possible.



The solution: develop a robust cybersecurity program

Every organization needs to have a comprehensive security program in place to protect its information assets and avoid penalties.

Given the above, organizations are often not clear on what a comprehensive cybersecurity program consists of. Technical systems alone are not enough to protect personal data. But there are a number of effective measures you can take to reduce cyber risks.

What is cybersecurity?

Cybersecurity consists of technologies, processes, and other measures that are designed to protect systems, networks, and data from cyber crimes. Information security is a broader term that describes the processes, tools, and policies necessary to prevent, detect, document, and counter threats to information.

The three fundamental domains of effective cybersecurity are people, processes, and technology. All are involved in the best approach to effective information security: Identify the threats, vulnerabilities, and risks the organization faces, while forecasting the impact and likelihood of such risks materializing.

Once the risks, impact and likelihood have been determined, the organization should implement appropriate measures to mitigate those risks while balancing its business objectives against cost.

A robust cybersecurity program:

1. Is based on a risk assessment, not just a set of very expensive technical controls that don't consider underlying risks and how to most effectively treat them.

2. Considers not only cybersecurity risks but also risks to information in all its forms. People are often the biggest cause of a data breach, particularly when they face improper processes or lack of procedures.

3. Is based on the implementation of an information security management system (ISMS) – a centrally managed system for protecting the organization's data in one place.

4. Requires regular reviews, testing, assessment, and continual improvement in order to adapt to constantly evolving risks.

5. Has the support of the CEO and board, is communicated throughout the organization, and is ingrained in the organization's culture.

6. Protects the confidentiality, availability, and integrity of data.

7. Is able to recover quickly and contain damage in the event of a breach, which experts agree is now becoming a reality of doing business.

8. Lends itself to audits by an independent third party to establish whether the controls in place are protecting the risks it set out to mitigate.

AN ISMS is a systematic approach to managing confidential or sensitive company information – including consumer data – in a secure manner. From an ISMS standpoint, information should be protected on three fronts:

Confidentiality:

Only those who have permission should be able to access protected information.

Integrity:

Information should be current, accurate, and protected from unauthorized modification, destruction, and loss.

Availability:

Information should be readily available to authorized persons as necessary.

ISO 27001 supports the above qualities, and is the international standard that describes the requirements for implementing an ISMS.

What is ISO 27001?

ISO/IEC 27001:2013 (ISO 27001) is the international standard that describes the requirements for implementing an ISMS. Accredited certification to ISO 27001 demonstrates that your company is following accepted information security standards, and delivers an independent, expert assessment of whether your data is adequately protected. ISO 27001 is supported by its code of practice, ISO/IEC 27002:2013.

What is involved in implementing an ISMS?

Implementing an ISMS is a serious undertaking – strategic and operational, while taking the entire organization into consideration. People, processes, and technology are involved in ensuring full coverage at all points where information may be compromised.

IT Governance has designed a nine-step approach to ISO 27001-compliant ISMS implementation, which its consultants have used in hundreds of successful cybersecurity projects globally.

Please see the next page for a brief breakdown of each of the nine steps.

	Nine steps to successful ISMS implementation	Key deliverable(s)
1	**Project mandate:** Project leaders establish the need for an ISMS. Determine program objectives, budget, timeline, and upper management support.	Project initiation document (PID)
2	**Project initiation:** Finalize information security objectives and outline project governance structure in a PID extension, which feeds into the Information Security (IS) policy. Designate a project team and steering group. Loans, advances and investments.	Four-tier documentation structure
3	**ISMS initiation:** Finalize information security objectives and outline project governance structure in a PID extension, which feeds into the IS policy. Designate a project team and steering group. Loans, advances and investments.	ISMS scope key arrangements
4	**Management framework:** Clearly define ISMS parameters and context while examining stakeholders' interests. Account for remote workforce.	Penetration testing
5	**Baseline security criteria:** Draw up requirements with corresponding measures and/or controls for the business to function. Ensure you're meeting legal security obligations.	Core security requirements IS legal requirements audit
6	**Implementation:** Build actual security controls to protect information assets. Evaluate competencies across business functions, including business continuity, risk management, etc. Enforce employee-wide IS policy awareness.	Likelihood-impact matrix Statement of Applicability Risk treatment plan
7	**Implementation:** Build actual security controls to protect information assets. Evaluate competencies across business functions, including business continuity, risk management, etc. Enforce employee-wide IS policy awareness.	IS policy awareness plan
8	**Measure, monitor and review:** Integrate processes that feed into the continual improvement cycle. Determine how often certain processes are used.	Internal audit Management review
9	**Certification:** Enlist an independent, external certification body that is accredited by a member of the International Accreditation Forum (IAF) for ISMS evaluation	Evidence of a functional, active ISMS

For a more in-depth look into these nine steps, download our free green paper: Implementing an ISMS – The nine-step approach

What are the benefits of obtaining accredited certification of the ISMS?

Accredited certification (registration) to ISO 27001 sends a clear message to existing and potential clients that you have implemented an ISMS that adheres to best practice. Compliance with ISO 27001 could help to seal the deal as security concerns mount in light of data breaches that have hit high-profile companies, including Equifax, Morgan Stanley, and Home Depot. Best-in-class brands such as Google, Microsoft, and Verizon have achieved accredited registration to ISO 27001.

ISO 27001 is a global standard, and accredited ISMS certification will help you to communicate your secure value proposition to target markets around the world. Increasingly, international markets demand ISO 27001 registration to do business with them (Japan and India have made it a legal requirement).

How we can help

IT Governance is a global expert in cybersecurity and data security compliance. Our team led the world's first successful certification to the ISO 27001 standard.

We offer the full range of products and services to help you implement the Standard and achieve full compliance, by either following a DIY approach through books, training, toolkits, or DIY packages, or by outsourcing the entire implementation project to our specialist consultancy team.

ISO 27001 products and services	
Books	**Policies and procedures**
Training and qualifications	**Staff awareness programs**
ISO 27001 family of standards	**Software**
Implementation consultancy	**DIY packages**
Penetration testing	**Free resources**

Whatever the nature or size of your problem, we are here to help.
Click the button below to request a call.
One of our experts will get in touch as soon as possible.

Speak to an expert

IT Governance Ltd

Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park, Ely,
Cambs. CB7 4EA. United Kingdom.

t: + 1 877 317 3454
e: servicecenter@itgovernanceusa.com
w: www.itgovernanceusa.com

/ITGovernanceLtd /ITGovernanceLtd /ITGovernanceLtd