

Ensure that Your IT Policies and Procedures Comply with Data Security Standards

By Mathieu Gorge

Founder and CEO of Vigitrust

Why should your organization be concerned about data security standards?

In the wake of the financial crisis which hit global markets at the end of 2008 and in the midst of economic pessimism, governments worldwide are taking action to restore confidence in the financial markets. What this typically involves is a mix of measures including nationalization of financial institutions, appointment of government heads on the board of key banks and new regulations aimed at ensuring that financial markets are regulated and watched carefully such that filed accounts actually provide a true reflection of the financial situation of organizations.

In practice this means that organizations will be asked to demonstrate that the "workings" of any financial statements are accurate, thus meaning that IT systems used to compile, process, store and transmit financial information are secure. In other words, emphasis on compliance with legal and industry data security and corporate compliance mandates is likely to increase in 2009 and 2010. With GLBA, SB 1386, PCI DSS, SEC 17-a, EU Data Protection to name but a few, did we really need more regulations and how are we going to deal with increased scrutiny on data security?

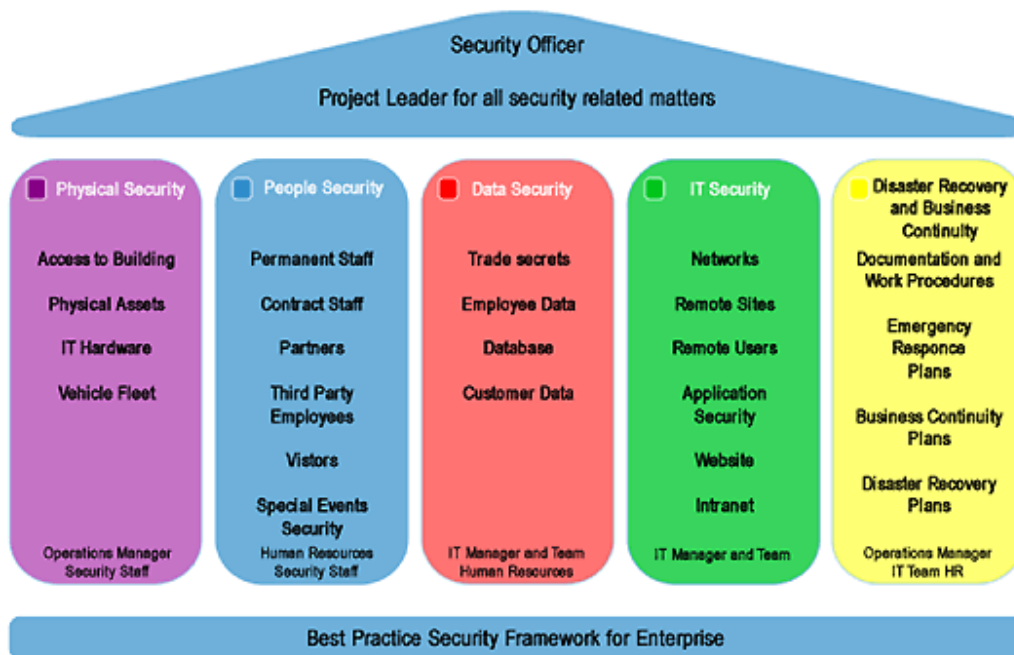
The usual best practice approach is to focus on implanting a framework to manage information and overall data security which involves policies and procedures, technical solutions, as well as user awareness. Technical solutions are typically well understood by compliance people, IT staff and senior management. It is obvious what AV or Anti-Spam does, why we need firewalls or why encrypting data adds value to the security of an organization's data. However what is not always obvious is the fact technical security solutions are only as strong as the policies and procedures (P&Ps) that they help implement and that users need to be aware of P&Ps in order for the overall framework to work.

So which Policies and Procedures do I really need to implement in my organization?

The first thing to do is to understand what legal and industry frameworks your organization needs to comply with. This informs the type and number of P&Ps you need to have in place.

Over the past 5 years, VigiTrust has helped numerous organizations with their legal and industry compliance efforts. Based on this experience, the VigiTrust Five Security Pillars Framework™ was created to act as a very simple and easy to implement framework for security compliance. The framework is based on the assumption that an organization needs to be fully aware of its physical environment and of who is allowed into and out of this environment be it at a physical level (e.g. who can come into the building, can anyone access the server room, can anyone access the boardroom area, does every staff member have full access to all servers or is this restricted on a business need to know). It also builds on the fact that most organization tend to have either a loosely established or a fully document data classification setting out which data can be published in the public domain and which data needs to remain company confidential or be restricted to senior management only. It is at that stage that a series of P&Ps need to be designed and signed off by senior management. Once they are set in stone, technical security solutions can be implemented to enforce the P&Ps. Finally, crisis situations need to be catered for and it is vital that Emergency Response Plans (ERPs), Business Continuity Plans (BC) and Disaster Recovery Plans (DR) cover the over four other pillars. This is key to ensure that changes to the physical environment, staff members, data security levels and technical environments are designed in such a way that mission critical systems are always available for the right staff as well as external people (customers, partners) to have access to the relevant data in accordance to data security classification.

The VigiTrust Five Security Pillars Framework™ can be represented as follows:



It is worth noting that in order for any security framework to be successful, there must be a designated person ultimately in charge of security. In fact, most security mandates require a security officer to be appointed. The EU Data Protection regime requires a main Data Controller to be appointed whilst frameworks such as ISO 27000 series require a full security officer and also recommend a security team, sometimes implemented as a focus group to be put in place.

"The Key thing for your compliance program is to use a common framework across your enterprise which will allow you to comply with multiple legal and industry frameworks in international jurisdictions thus addressing both operational security as well as the CIA concept (Confidentiality, Integrity and Availability)"—Mathieu Gorge, CEO VigiTrust

In terms of policies and procedures, the main challenge for organizations is to understand which need to be in place, when to roll them out and how to maintain them up to date. In that respect, it is key for organizations to ensure that there is a framework to establish and maintain policies and procedures in the first place. Whilst this could be seen as a framework within a wider security framework, it will make much more practical and effective to manage security P&Ps. One key piece of advice is to make sure that a document management and version control P&P is put in place clearly stating who the owner of each policy is, how often they need to be updated or reviewed and what the policy "governs". This will inform how the rest of the policies and procedures are to be designed and managed. As a tip, it is worth noting that frameworks such as ISO 27001 actually start by requiring this element to be addressed before looking into more specific physical and logical security aspects. Indeed, it requires that the organizations specifies the scope of what the ISO 27001 Information Security Management System (ISMS) is to cover and then requires a versioning and control mechanism to manage the P&Ps which are at the core of the overall ISMS.

As security pre-auditors for PCI DSS and for ISO 27001 Compliance helping organizations prepare for the official accreditation bodies such as Qualified Security Assessors (for PCI DSS), VigiTrust auditors will typically benchmark organizations against best practice security and will ensure that they have the following security policies and processes in place. As such all available documentation and technical solutions in place are benchmarked against what should be in place in accordance with ISO 27001 and PCI DSS as well as the VigiTrust Best Practice Security Framework. Here follows a sample of some of the items covered in each area by VigiTrusts' library of policy & procedures.

Physical Security

- Building Alarms
- Office Access
 - Corporate Identity Card and/or Access Management Policy
 - Key Management Policy

People Security Policies and Procedures

- Employee Background Checks (depending on applicable laws)
- Reference checking policy
- Leavers Policy

Data Security Policies and Procedures

Legal Framework Policies and Procedures

- Data Protection Compliance Policy (EU Data Protection—where applicable)
- Intellectual Property Rights (IPR) and copyright strategy
- Third Party Consulting Contracts Security Reviews
- Spam handling procedures (incoming and outgoing Spam from a legal perspective—e.g. Spam Can Act and equivalent)

Data Security P&Ps (Operational and Security Aspects)

- Data Classification Policy
 - Public
 - Confidential
 - Highly Confidential
- Phone Usage Policy
- Cross Skilling policy

Additional Data Security P&Ps

- SDLC Policy—Security during project lifecycles

IT Security Policies

Documentation Work, Support and Shared Knowledge Base policies

- Ecosystem Diagrams
- Network Diagrams

IT Technical Solutions Security P&Ps

- Generic Security Architecture and Network Scalability Strategy
- Systems Management & Security Event Management P&P
- Firewall
- Anti-Virus and Anti-Spam
- Green IT Strategies

Disaster Recovery and Business Continuity

- Business Continuity (BC) and Disaster Recovery (DR) related policies
- Emergency Response Plans

The above list is only a sample, however it's worth noting that all security best practice frameworks typically require organizations to really focus on the following P&Ps:

- Documentation work including version control and change management as well as ecosystem diagrams allowing you to regain control of the security of your environment and to demonstrate your proactive security strategy to auditors and customers & partners alike
- AUP: Acceptable Usage Policies covering all the corporate communications tools you need in order to conduct your daily business
- A Business Continuity Plan and a Disaster Recovery Plan to ensure that all of your mission critical business applications are always available to your critical staff members and business functions.

Final thoughts

Whilst this document only offers a brief introduction into the value add of Policies and Procedures for the overall success of security program as part of a GRC strategy (Governance, Risk Management and Compliance), businesses would be urged to ensure that they at least consider an approach based on the Five Security Pillars Framework or equivalent in order to ensure that policies and procedures are "alive and kicking" and help the business to grow and remain secure. Business is getting tougher and so should your security infrastructure!