PECB *Insights*

PROTECTING PERSONAL DATA

ISSUE 04 / January **2017**

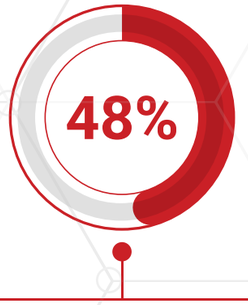
When Standards Matter

WHICH SIDE ARE YOU ON?

OF U.S. INTERNET USERS WORRY ABOUT THEIR PRIVACY ONLINE

AVOID COMPANIES THAT DO NOT PROTECT THEIR PERSONAL INFORMATION

ARE CONCERNED ABOUT DATA BREACH AND LOSSES



ARE CONSIDERING CHANGING THEIR INFORMATION SECURITY MANAGEMENT MODEL

"I don't mind if my information is purchased without asking me"

34% Stated that businesses must review their information consent processes

56% Reported that third party information sharing should be limited

73% Think banks shall have affirmative consent regarding information selling

CONSUMERS

Source: 2016 IDG Enterprise Cloud Computing Survey

78% BIG DATA ANALYTICS WILL CHANGE BUSINESS MAKING THE NEXT THREE YEARS

51% USE BIG DATA TO IDENTIFY INFORMATION SECURITY INCIDENTS

13% AUDITED TO ENSURE LEGAL COMPLIANCE

ORGANIZATIONS

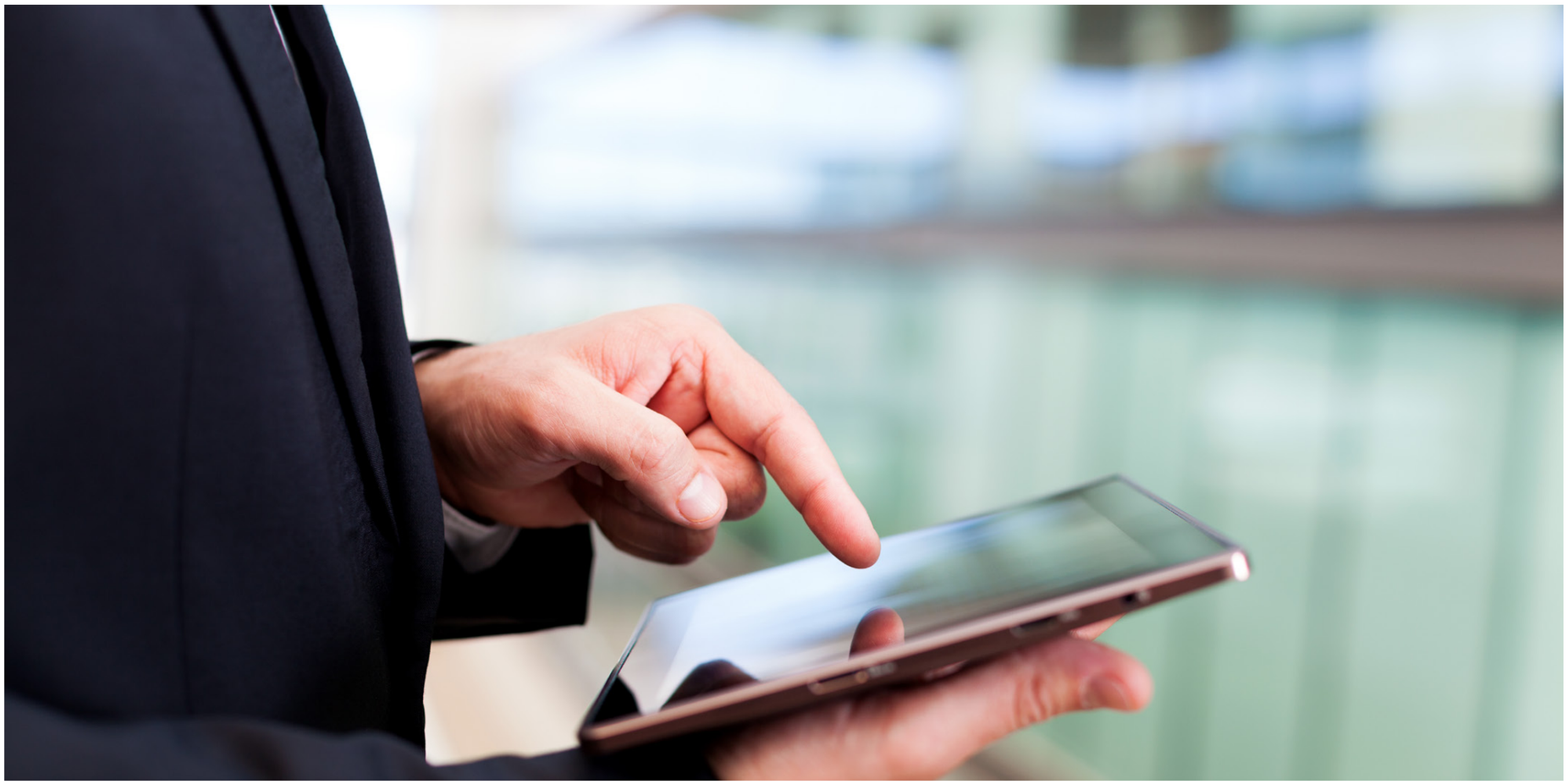
The Information Security Industry

What's the Status?

Information handling is definitely being presented as a very concerning factor in data protection. Additionally, almost all countries have developed information and privacy protection acts to the convenience of their population. Moreover, protecting intellectual property has been a benefit to which organizations are continuously benefiting from. Hence, Information Security programs and legal regulations are mandatory to be performed at not only public institutions but also private organizations.

Parallel to technological development, both trade and logistics have been majorly progressing due to the new online channels of commerce. Though, with these developments, both information handling and security have been constantly driving the online customers to often stop the purchase due to doubt of the online platforms. At the same time, as the online customer is getting more aware of the importance and misuse of their personal information online, they are asking for more and more legal rights and competences over their personal data. Consequently, organizations experience major losses, in both financial and reputational aspects.

However, it is important to highlight that the governments and policy makers are struggling to catch up with the hacking and data breaches development. As an extremely multiplicative incidence; data breaches and technological innovation are being found difficult to cope with in the emerging nations. In addition, lack of transparency from the governments and business entities about the use and reproduction of personal data are definitely holding back.



The United States has implemented the legal protection of privacy since the late 1800's in their common law system. However, their privacy laws have advanced majorly since those times. Currently, the United States has in place specific privacy laws with respect to various sensitive consumer and citizen data at risk. Including financial information, medical information, legal, telephone, internet and various electric communication records, privacy laws bind to protect our position in the society as well as the online environment. As with most states of the world, disclosing such information is prohibited and considered a criminal act. Thus, we should seriously consider complying with necessary legal requirements.

Depending on the industry, the rate of information security spending varies from one organization to another. Information security spending was predicted to reach nearly $82 billion in 2016, increasing at a rate of close to 8% from 2015. Nevertheless, this leads us to think through the continuous growth in information security spending due to fast technological advancements, we are expected to see 90% of the organizations will implement various DLP software by 2018.

ARTICLE SERIES

MATCHING INFORMATION SECURITY AND AGILE VOL. 1

FOUR REASONS WHY TRADITIONAL INFORMATION SECURITY FAILS IN AGILE ENVIRONMENTS

While agile development is going mainstream, information security is having difficulties to keep pace with such short-term planning perspectives and instant changes in strategies. The result of this struggle is that new systems are insecure, or that they are loaded with point solutions for security.

What is so hard about security in agile environments? In this article, we examine what makes information security fail with agile, while in future articles we will propose solutions for it and present a model to integrate information security into an agile development process.

So, what is wrong with classical Information Security in relation to agile?

This has to do with the common way of working within security management. Popular information security frameworks (such as ISO 27001) use a top-down approach: They emphasize that policies, processes and generic technical controls need to be in place to make sure an organization is in control of its information security. Once all of that is in place, projects can start building on this security foundation and use security management services. This works well in the top-down projects that follow the waterfall model, with clearly defined transition moments and deliverables. Essentially, information security is often addressed at the start and end of a project.

Agile, however, follows a different model; it uses a risk-based approach for developing in an incremental way, using short development cycles called sprints. A sprint is small enough to be manageable and it forces the product owner to set priorities; and all new feature requests are collected in the backlog. For each sprint, a selection of requests is made, based on business value, urgency, ease of implementation, customer requirements, and etcetera. If a feature or requirement is too complex or will take too long to implement, it may be broken down into smaller bits and implemented in a series of sprints. Test results from previous sprints are fed back into the next sprints to facilitate continuous improvement while performing sprints.

So where do things go wrong?
Traditional security assumes that:

1. THE PROJECT TEAM TRANSLATES GENERIC SECURITY REQUIREMENTS TO APPROPRIATE SECURITY CONTROLS
2. THE TEAM HAS TIME, SKILLS AND TOOLS TO IMPLEMENT THE CONTROLS PROPERLY
3. DURING THE DEVELOPMENT PROJECT, THERE IS SUFFICIENT TIME AND MONEY TO CONDUCT A SECURITY TEST OR TESTS AND PROCESS THE FINDINGS
4. SUFFICIENT TIME IS AVAILABLE TO ADDRESS THE SECURITY RISKS FOUND DURING THE PROJECT AND TEST

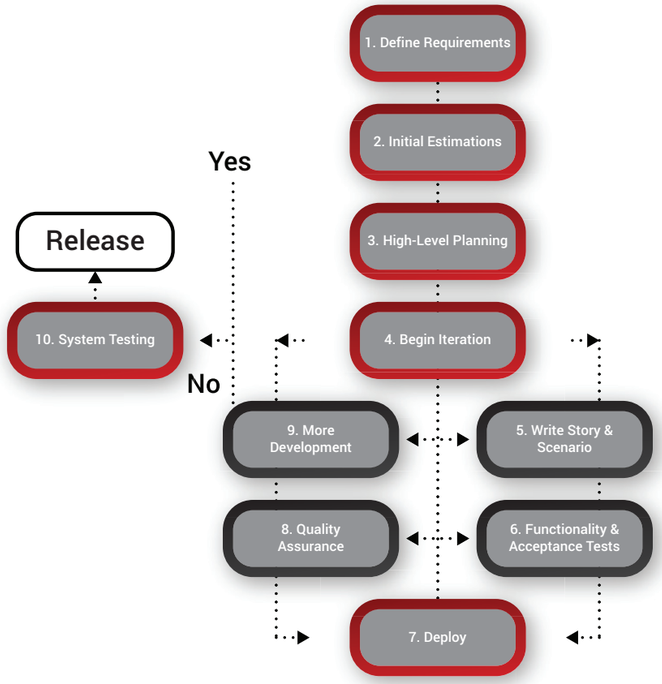
These assumptions do not hold up in an agile environment.

1 First, the product owner has other priorities than to translate security requirements to controls. Time is of the essence in an agile approach and most, if not all, resources are dedicated to building the next iteration of building blocks required and creating business value.

2 Second, the development team may lack the state of mind, expertise, and experience to implement security controls. Developers may not be aware of some of the vulnerabilities that could be present in the building blocks and may lack the proper training for developing secure code.

3 Third, there is no traditional test phase, where the product is frozen, in the project where all functional and non-functional requirements can be tested and issues can be fixed. The system is developed and released in a flow of small, incremental cycles. Each cycle determines what is developed and delivered in the next cycle, and the 'predictability' of the project is perhaps two or three cycles down the road. More often than not, different iterations run in parallel and they meet somewhere further down the road. Security testing is limited to the products that are available in the sprint and security management is often not able to adapt to that dynamic.

4 Fourth, there is a cultural issue as well. Not all of them, but most developers do not get warm fuzzy feelings when you mention the term 'information security'. They know that it creates a lot of overhead when they are required to incorporate security controls. There is no direct benefit (i.e. functionality) in implementing security controls. However, it can take up considerable development time and prevent developers from implementing other features and functions.



This article is the first in a series written by the authors to explore the options for embedding information security into an agile development strategy. In the next article, they are going to present solutions and a model for agile security.

PECB

Information Security is becoming increasingly important for nowadays organizations in one hand. On the other hand, certifying against it is oriented towards being a mandatory requirement for both the organization and individuals practicing security. Competently, PECB ensures valuable training and certification against ISO 27001 while expanding individuals' abilities in responding towards various threats and vulnerabilities.

ABOUT THE AUTHOR

Arthur Donkers is highly experienced in Computer and Network Security, specializing in Information Systems Security, Information Systems Security Architecture, Information System Security Management, Auditing Information Systems, and Ethical Hacking. Mr. Donkers has employed his expertise in various security organizations, starting at BSO (now ATOS), Umbrella (now Akisgorta), KPN Telecom, Dutch Ministry of Defense, Euroclear, Informatie Beheer Groep, Achemea, Rabobank, Trustforce Security, Westland Utrecht Bank, ITSX BV, Gemeente Groningen, Warpnet, SOO Noord while currently being a partner at 1Secure. The industries worked in range to Telecommunications, Insurance, IT, National Defense, Finance as well as the Digital Government foundation through ICTU.

Pascal de Koning is a highly skilled professional on Information Security, Security Architecture, Software Development, PCI DSS, Identity Management, TOGAF, Network Security, Integration, Business Continuity, and IAM. As a Chairman of Security Services Catalogue project supported by OSA and a Chairman of the TOGAF-SABSA integration project at KPN Telecommunications, his expertise becomes of great value to provide.

KEY RISK INDICATOR

MEASURING THE SUCCESS OF ENTERPRISE RISK MANAGEMENT

Performance and risk indicators are essential business measurements that make a significant distinction to how organizations are governed. Thus, measurements provide insights in the way an organisational system operates using metrics that are translated into KPIs (Key Performance Indicators) and KRIs (Key Risk Indicators).

When metrics measure the achievement of a desired state they become performance indicators. A KPI expresses the achievement of a desired level of results in an area relevant to the organization, it shapes its behaviours. For example, air pollution may be just a metric, but for an organization that is concerned by reducing the environmental impact of its production process, it becomes an important KPI for their HSSE department.

With metrics providing early warnings regarding an increased risk exposure in certain areas, they become key risk indicators. By monitoring KRIs, the organization identifies the problem expressed by them early on. They can take a proactive approach of mitigating risks before the event occurrence and have more serious consequences. For example, a large percentage of customers in financial difficulties can be a KRI as it indicates how large the company exposure is toward its clients. Many customers with financial problems can affect the cash flow of the organization. Essentially, it is a key enabling structure and active relation among risk management, strategy and target setting. Every organization follows different aims to add value, and should generally recognize the acceptable level of risk in doing so.

Below is an example of KRI classification proposed by Dr. A. Chapelle that can help the organization to choose the most appropriate indicators;

Indicator Type	Description
Exposure Indicators	Any significant change in the nature of the business environment and in its exposure to critical stakeholders or critical resources. Flag any change in the risk response.
Stress Indicators	Any significant rise in the use of resources by the business, whether human or material. Flag any risk rising from overloaded humans, machines or systems.
Causal Indicators	Metrics capturing the drivers of key risks to the business; the cause of the cause of the incidents. The core of preventive KRIs.
Failure Indicators	Poor performance and failing controls are strong risk drivers. Failed KPIs.

Therefore, good KRIs act as an early warning system giving to management sufficient time to consider range of choices to prevent a much bigger problem from happening. They bring attention to issues and speed up decision making before those bad consequences start to pile up.

What do we have to bear in mind when designing and reporting KRIs?
The most common characteristics of alarm systems is that people don't respond properly because they don't know what the indicators mean, they don't know what their significance is. If a KRI is indicating there is an issue and no one cares or pays attention or has any belief in its value, then there is not that much point putting the work in to collect the data and make the report in the first place.

To ensure that the KRIs can make a real difference in your organization and will not create false assurance, here are the features to identify, select and design effective KRIs:

1. **Early warning sensors**
   - Signal changes in risk: increase in probability or in impact, before the risk materializes
2. **Must address risks, not events**
   - KRI are metrics capturing risk drivers or proxies of these risk drivers
3. **Specific to each activity:**
   - Specific to each risk, and to specific weaknesses and culture of different institutions.
   - One size does not fit all
4. **Best identified via data analysis and experience**
   - Business experience complements lack of data
   - Data analysis: to confirm business intuition, and uncover other effects
5. **May need heavy data collection**
   - Trade-off to operate between the value of information collected and its cost of collection.
   - Better if automated
6. **Must be easy to use and timely**
   - Should match the cycle of the activity
7. **Must help business decision**
   - The rules of reporting apply to KRIs: only keep reports that do influence business decisions
8. **Thresholds linked to risk appetite**
   - Typically, lower threshold for core business (low risk), but not always
   - 100% (or about) target reliability does not mean 100% for all indicators; but only so collectively
9. **Must be back tested for validity**
   - How do you know it works? An essential question in risk management

With all above in place, a useful and proven scheme for effectively managing KRIs to streamline risk management and align it to best practices is established. KRIs are like any metrics, they are read by human beings, we may systematize them, load them with clever analytical data, but actions are taken by people. There is a need to reduce or eliminate these biases in adopting an internationally recognized standard such as ISO 31000, which drives the most relevant best-practice from organizations worldwide. It provides principles; a framework and a process to implement a risk management suite allowing the identification, the selection and the design of appropriate KRIs.

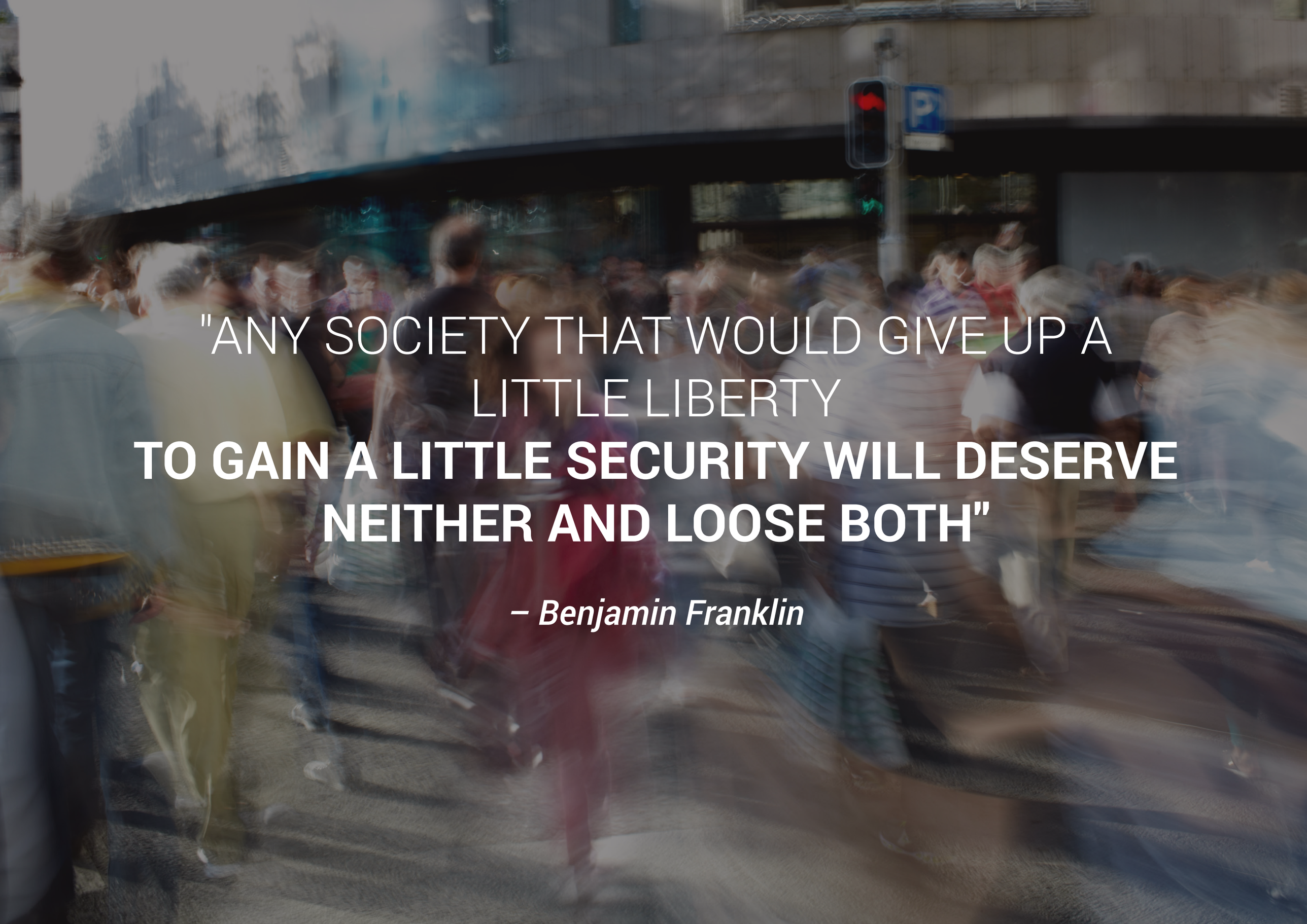
Moreover, with due cognizance of its own internal and external contexts, an organization must recognize the applicable and relevant obligations and should put into practice a system of controls to attain compliance. Additionally, ISO 31000 distinguishes the significance of feedback by means of two mechanisms: "communicating and consulting" and the "monitoring and reviewing" of performance. Communicating and consulting ensure the engagement of relevant internal and external stakeholders while monitoring and reviewing guarantee that the organization observes its risk indicators without bringing the false sense of assurance.

PECB

Implementing various risk assessment methods and Key Risk Indicators does clearly emphasize upon the success of your organization. Measuring risk also expedites undertaking preventive actions. Additionally, complying with ISO 31000 raises the bar of success in individuals implementing the standard in conjunction to having Risk Management Systems in place. Certifying against ISO 31000 through PECB ensures worldwide recognition and distinctive training.

ABOUT THE AUTHOR

David Lannoy is a Senior Enterprise Risk Manager in a global telecommunication company and an experienced freelance risk trainer. He has vast experience in Risk Management gained over 15 years of working in various sectors including transport and finance. He is a regular guest lecturer and master thesis supervisor in well ranked Business Schools. Due to this valuable experience and academic track record, he has been able to join The Institute of Risk Management in London as a Specialist Member and has also become a Certified ISO 31000 Risk Professional and Certified PECB Trainer.


"ANY SOCIETY THAT WOULD GIVE UP A
LITTLE LIBERTY
TO GAIN A LITTLE SECURITY WILL DESERVE
NEITHER AND LOOSE BOTH"
– Benjamin Franklin

GLOBAL SUPPLY CHAIN
ARE WE HEADING IN THE RIGHT DIRECTION?

The recent supply chain disruption experienced as a result of the Hanjin Shipping Co.'s financial and legal troubles is neither the first, nor unfortunately will it be the last case of the supply risks encountered these days.

Thus, every organization must consider an integral element of doing business in today's global economy. Seeing that an ongoing series of major disasters over recent years, such as the earthquake and tsunami in Japan; flooding in Thailand; fire at a Bangladesh factory that resulted in the loss of 100 garment workers; a dock strike in Belgium; droughts in Brazil; and ongoing political turmoil. In addition, there are many supply chain disruptions caused by events that are so localized, they are not reported by the media or noticed outside the immediate area. Consequently, fragile economies throughout the world must raise the level of concern.

Bottom line, that the supply chain risk is always present, and must be managed, is a business fact of life.

Regardless of the size of an organization or the product or service it delivers, the more global the supply chain, the greater the number of risks, and the greater the potential for supply chain disruptions.

Many companies have made impressive strides over the past several years as they have developed and implemented programs that evolve the management of supply chain risk from a reactive approach to a comprehensive, from a proactive approach to mitigating and managing supply network risk. For some this has required a significant investment of financial and human resources to improve and expand existing continuity programs. For others, it has meant starting from scratch to identify and address their supply chain vulnerabilities.

Whatever the starting point, questions are often asked regarding a comprehensive business continuity program. "What is enough?" "Are we heading in the right direction?" "How can we measure our business continuity management capability against best practices?" "What are the expectations of interested parties?" What separates the most mature and robust programs from the rest?

We can begin by asking ourselves some rudimentary questions based on accepted best practices and standards. What is the level of executive involvement and support? Is supply chain continuity integrated with other enterprise risk management/continuity programs? In the case of an existing program, how often is the program reviewed and updated?

Primarily, an initial measure of an organization's supply chain continuity management capability can be based on asking how true the following statements are for the organization:

- The organization has selected and adopted a business continuity standard such as ISO 22301 that encompasses its supply chain.
- Supply chain business units participate in the company's business continuity program and are fully represented at the business continuity planning table.
- **Resources** - people skills and hours and financial means - are made available to adequately support supply chain continuity/ risk management program development, implementation, and maintenance.
- Supply-chain-related business continuity responsibilities are included in job descriptions, and **business continuity knowledge, experience, and certification** are taken into account when hiring and promoting.
- Employees with supply chain continuity responsibilities are provided with the necessary business continuity training, fully participating in exercises and tests.
- As part of a risk assessment process, the supply chain has been mapped from raw materials through delivery to the customer, to identify and quantify the risks and appropriate risk treatments (mitigation).
- Selection of all suppliers, outsourcing companies, and contractors – upstream and downstream - includes quantifying the associated risk and the business continuity capabilities of the applicants.
- Supplier relationships are developed and cultivated. All suppliers are made aware of business continuity requirements and expectations, and are encouraged to develop a robust business continuity program based on an accepted standard. Joint business continuity planning conducted with key suppliers is mutually beneficial.
- Post-contract, suppliers are monitored for "red flags" and negative changes in risk factors such as their financial stability, significant changes in management approach, a decreasing level of quality, or lag in deliveries or response time to inquiries, to avoid today's dream supplier becoming tomorrow's nightmare.
- A process is in place to monitor the horizon for new risks and threats, thus avoiding addressing only those supply chain disruptions that have occurred in the past.
- There is a cyber-security awareness program that includes securing supply chain internal data and information systems, and collaborates with third parties who provide products and services to the company.
- The company has in place trained continuity teams, strategies, plans and adequate resources to respond when there is a disaster or significant supply chain disruption.

Using this checklist will provide an indication of the sufficiency of the organization's supply chain continuity program and capability, gauge its progress, and identify areas for improvement; however, it is not by any means a replacement for a comprehensive assessment. To fully evaluate how closely the program aligns with organizational policies and objectives, regulatory requirements, and the selected standard, (e.g., ISO 22301), – and an unbiased accounting of strengths and areas needing improvement, requires a comprehensive review or an audit.

Regardless of the current level of program maturity, making supply chains risk resilient must always be a work in progress. Once the initial continuity planning objectives have been achieved, there needs to be a cyclical process of continuous improvement to ensure that the needs and requirements of the organization and its stakeholders are met. Review your Business Continuity Plans. Identify and mitigate your internal and external supply risks. Develop and implement workable strategies and plans to manage supply chain disruptions and disasters.

Presently, supply chain environment is characterized by a growing realization and understanding that some of the major risks an organization faces may come from its supply chain. This realization comes with an undeniable need to identify, mitigate, and when possible, eliminate these risks, and to develop robust strategies to continue with steady business operations when a significant disruption does occur. Moreover, in today's precarious world, supply chain continuity relies both on internal capability and wisely selected and carefully nurtured supply chain partnerships, creating a firm foundation for both the organization and its suppliers to address supply risks, cooperate during a crisis, and realize greater resiliency.

PECB

As the complexity of global transportation is becoming more difficult to manage, it is at the same time being threatened by unexpected events like; natural disasters, theft, and even weak preservation of goods during transport. With all resulting to losses in organizations either tangible or intangible value, it should become primary to organizations to implement Business Continuity Management Systems. Ensuring integrity, quality, and recognition, PECB will undoubtedly facilitate your ability to protect and improve the supply chain in your organization through prime quality training and certification.

ABOUT THE AUTHOR

Betty A. Kildow, a consultant with more than twenty-five years of business experience, has specialized in business continuity, disaster recovery, and emergency management consulting for more than two decades. Ms. Kildow is experienced in conducting business continuity reviews and audits, risk assessments and business impact analyses, developing emergency management, business continuity, and disaster recovery strategies and related plans and procedures, designing and conducting exercises and tests, and coaching those newly assigned to disaster recovery and business continuity responsibilities. She also taught a business continuity/disaster recovery class in the Massachusetts Maritime Academy's Emergency Management Master's Degree Program from 2013-2015.

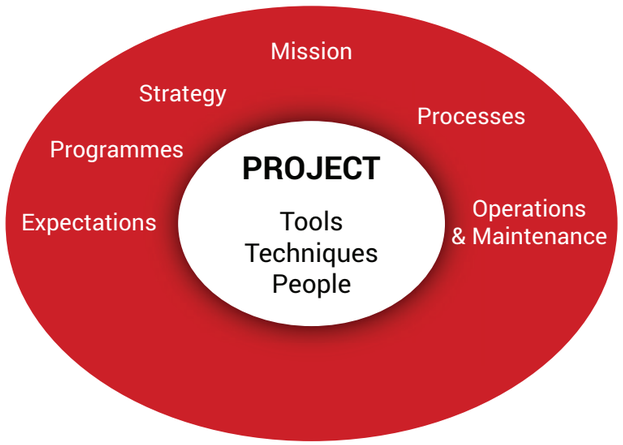
INFORMATION SECURITY IN PROJECT GOVERNANCE

INCIDENTS AND PREVENTIONS

Worldwide there are several reasons for project start-ups, but what are the real reasons behind it. Another question to be asked here is "is there enough attention for Information Security in projects"?

The drawbacks of information security are both project and business risks. Referring to the investigation of Price Water House Cooper we may notice a 48% increasing rate of incidents, there are 117,339 Information Security incidents a day summing up to a yearly cost of 42,8 million. Additionally, the estimated damages world-wide peak to 2,7 million dollars for each incident. These figures mark a decrease of as much as 34% since last year! Thus, the urgency of companies comes down to how they can strengthen Information Security in the daily business and projects, by also eliminating 'security leaks' in the scope of Project Governance. Commonly Businesses do not become aware of such issues related to the Project Governance. In other words, the management becomes so occupied protecting the house and forgets the barn or even the new building in progress.

ISO 27001



For preventing vulnerabilities of Information Security in daily basis you may use ISO 27001 as a tool to increase Information Security within your organization. However, for Project Management as a temporary project organization you can concentrate on implementing the sub norm of ISO 27001, namely 6.5.1. These sub norms order security to be integrated in the project control mechanism as a part of project management and their processes.

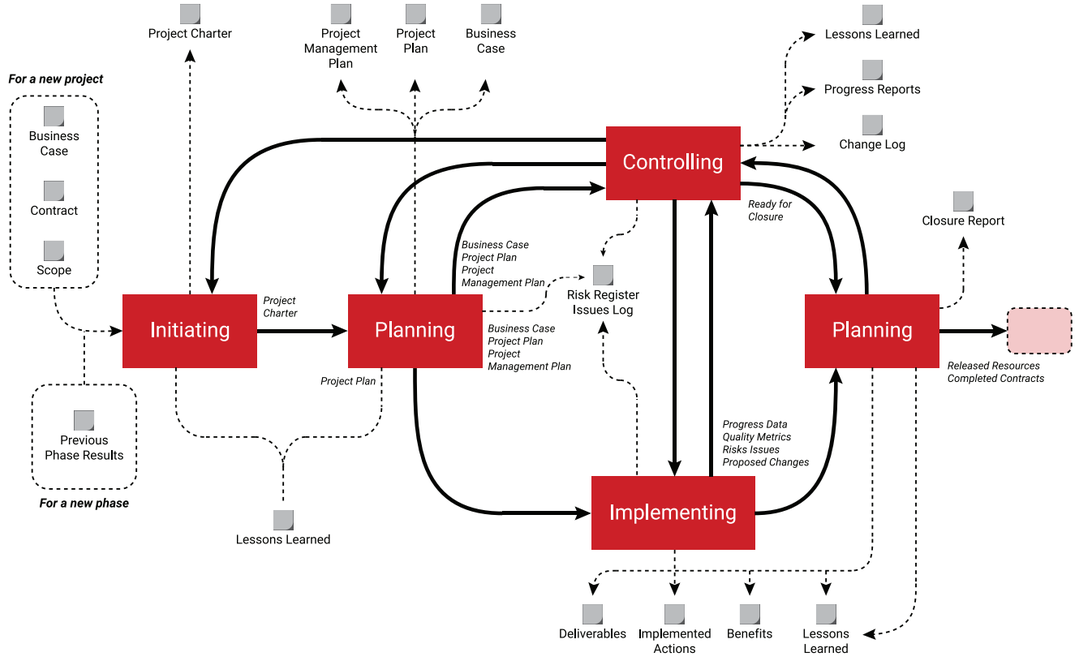
For effective Project Governance Security you must imbed:

- A Project Governance strategy, policy, a project plan/roadmap, project architecture and independent assurance;
- A temporary project organization with: ownerships, roles, accountability, responsibilities, and segregation of duties;
- A Project Risk Management team with: information of project risks, project management framework, risk assessment abilities, certification, training, education, dependence on project interfaces or key specialists, job changes and/or termination, knowledge sharing and project security awareness;
- Project configuration with: identification, maintenance of configuration items, configuration repositories and their baseline;
- Project Incident Problems and Incident/Problem Management; for incident escalation, and incident response on security issues;
- Project Change Management standard and procedures; For impact assessment, priority and authorization;
- Project development; A Project methodology for secure development, implementation;
- Project data classification; like ownership, classification, security requirements, exchange policy, disposal;
- Project Identity & Access Management for: Access rules, Access rights project administration, super users and periodic phase review of access rights;
- Project Security Management with: Company-Project security baseline in line with the strategy and policy, i.e.; authentication mechanism, mobile devices, teleworking, logging, security testing, surveillance, monitoring, threat and vulnerability, infrastructure resources, protection, availability, maintenance, project network security etc.;
- Project operations for: job processing, back-up and recovery procedures, capacity and performance management;
- Business continuity after closure of a project; business- and project continuity planning in line with continuous improvement (lesson learned), service level management and imbedding the Deming Cycle "Plan, Do, Check and Act".

ISO 21500 project management, in this case, is definitely advisable, being that, ISO 21500 is familiar with international project management and covers PRINCE2, International Competence Baseline (ICB), and PMI, it is also compatible with ISO 27001 and ISO group 55000, 9001 and 31000. This ISO family is compatible with: project control mechanism, policy, business governance, PDCA cycle control mechanism, screening, awareness, project and company continuity/hygiene. However, these are only some of the strongest points by adapting ISO 21500 in combination with ISO 27001.

Following this direction displayed above and ISO normalization with a 'practical handyman', both the internal audit department, and steering committee get a clear overview of the necessary steps for improvement in terms of security standardization and continuous improvement.

ISO 27001 / ISO 21500



Other international PM methodologies are also free to use, but, with ISO (International Organization for Standardization) you can prove:

- The difference between 'industry peers';
- Application for Bench Marketing, Best Value Procurement and European tenders;
- That procedures around 'Information Security in projects' are under control;
- The risks are known and that you can set-up or initiate the mitigations;
- Standardization;
- And that Quality is bound to increase through continuous improvement;

Correspondingly, in order for the Steering Committee to ensure a clear vision and involvement/sponsoring for ISO decisions concerning 'Information Security in projects', they need to answer:

- What quality level do we need for 'Information Security in projects?' What is the common or standardized ISO 27001/ISO 21500 level?
- What is our current situation presently?
- What are the steps to undertake for minimalizing the project and business risks?

Answering these questions is undoubtedly difficult. Managers do not always have enough overview or a consistent way of working. Therefore, they need professional consultants and tools to get a clear overview to address various issues happening to their organization. So, to a company, a proper project development plan supplemented by training and coaching may facilitate easier implementation.

Secondary ISO 21500 help you also to get more project maturity in project management.

During the last decades, several attempts have been made to determine the relationship between the maturity level of a company and project performance. After studying projects with 200 different organizations in 30 countries, it turned out that; the lower the maturity level of the company is, the higher the chance of project failure. Therefore, ISO 21500 project trainings help your organization to reach a higher level of maturity (read quality), which will undoubtedly lead to cost reduction up to an estimated 30%, as well as minimalize risk of project failure and naturally give more effectiveness of your projects.

Moreover, your company will certainly also benefit from:

- Proven, internationally recognized quality framework;
- Transfer of knowledge between projects and organizations;
- Integration with specific standards;
- Continuous improvement;
- Business continuity and business hygiene;
- Having a diagnostic tool for assurance and assessments.

If you have reached ISO 21500/ISO 27001 certification, then you should take a moment to celebrate this achievement! You need to tell your customers, vendors, employees and any other stakeholders of your accomplishment.

Tips and Tricks for Security.

It is recommended to get a clear overview about your network information while limiting Internet usage in your company or project environment for prevention from various outside risks and malwares. Make a choice of a Risk Management methodology i.e. ISO 31000; plan weekly, monthly, quarterly and yearly risk audits with several scenarios; invent external specialists and entrepreneurs; take a look on the outside, not only inside; What can happen? Which security development do you see? What is the news? Set-up and initiate a Security prevention team in your Governance with clear job descriptions about tasks, authorities, and responsibilities. Look at your internal company and project procedures if they are not too bureaucratic. Invest in professional and standardized company and project management information security. Adapt ISO 27001, ISO 21500 and ISO 31000. Be aware of the damage, costs if insecurity occurs. Create a permanent program for your employees and contractors. If they are not competent, screened and well trained they are your biggest risk. You need to create with the Human Resource Department, Business Manager and employee a Personal Development Program and awareness program of training.

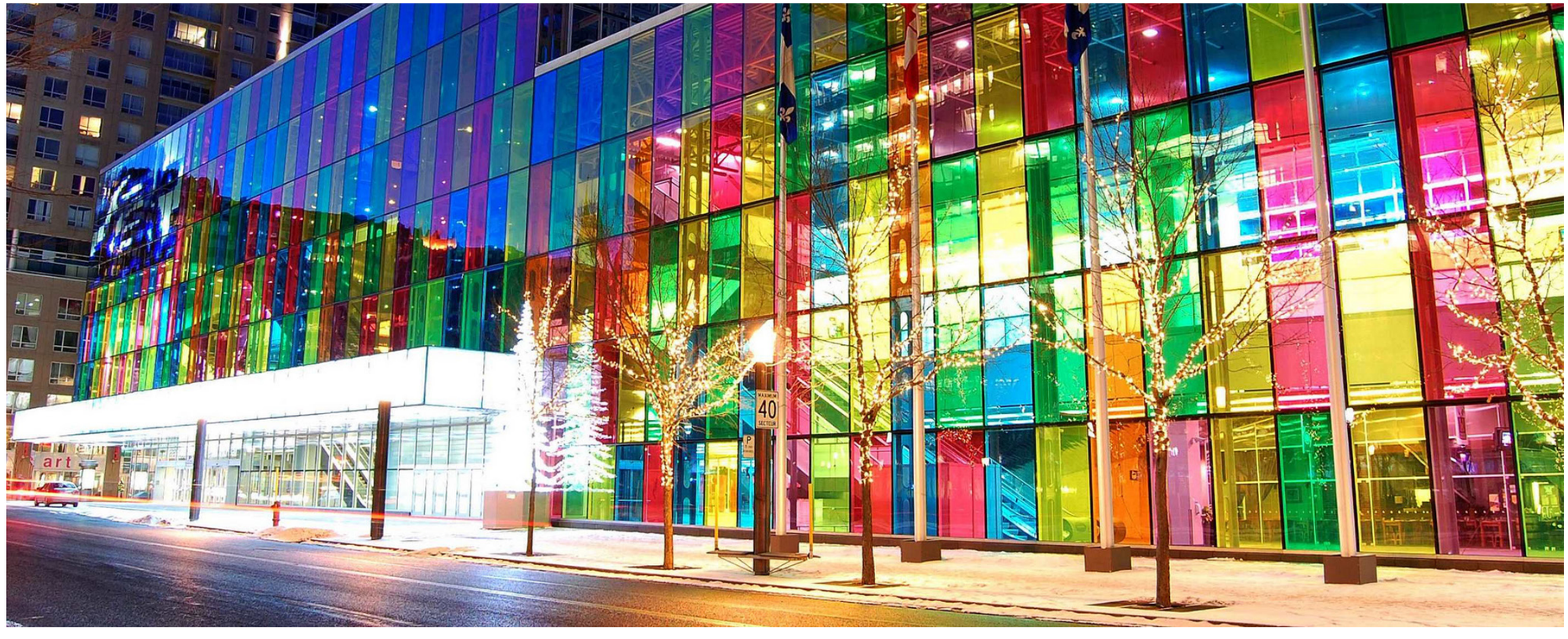
PECB

As a progressively harmful phenomenon to our society as much as the whole business environment, Information Security should not be neglected; regardless to the industry you are operating. Thus, we must give significant importance to the implementation of various Information Security frameworks. Likewise, implementing ISO 27001 and ISO 21500 in projects will confidently increase your project's likelihood of success. Harmoniously, PECB is pleased to offer you with thorough training on effective implementation while certifying you in both ISO 27001and ISO 21500.

ABOUT THE AUTHOR

John Roose can be characterized as Quality and Project manager with a rich experience in in the field of process improvements and project program control in a wide range of industries. Additionally, academic educations with professional certification (PRINCE2, IPMA, ISO21500, ISO27001, ISO31000) and experience have led to a successful track record in Project/Program management, Quality Improvement and Control mechanisms. As a Lead Auditor he emphasizes the need for a structured set-up including control (PDCA) mechanisms. Further, his experience has been applied at Damen Shiprepair Rotterdam BV, The Dow Chemical Company, KPN Telecom, Atos, Oce, Consumentenbond, Initial Nederland, Royal IHC, Centric, Deutsche Bank, Alstom, NedTrain, Sociale Verzekeringsbank, Rijksdienst voor Ondernemend Nederland, and NOVI.

INTRODUCING THE PECB STANDARDS INSIGHTS CONFERENCE



Announcing with gratitude, **The PECB Standards Insights Conference** will be held in **"Palais des congrès de Montréal" from June 29th to 30th, 2017.**

Attending this conference at the vibrant city of Montreal, Canada, will complement your professional opinions and reveal many future occurrences and disputable matters with respect to Management Systems.

Bringing together experts, practitioners, and influencers, the PECB Standards Insights Conference is organized to be attended in three different tracks, such as Information Security Management, Auditing & Management Systems, and Governance Risk and Compliance.

Emphasizing the value of information security in such a fast pace advancement era in report to technology is unquestionable. Additionally, various legal requirements and policies are contributing to the effort of strengthening information security within the organization, as much as are increasing social awareness. What is more, various cyber-attacks are jeopardizing information security at the state level, causing severe damages to national security. Therefore, this track will develop discussions on all of the abovementioned challenges, while emphasizing upon the innovative solutions that can be provided.

Establishing a strong internal auditing culture within the organization is mandatory to continuously improve. As a result, implementing a total quality culture would come as a result of effective control and unbiased attitude for improvement. Correspondingly, audit preparation, performance, reporting, and closure will precede this specific conference track while revealing the importance of certified and competent and professional institutions to perform auditing. New technologies and frameworks will also be presented during this conference track.

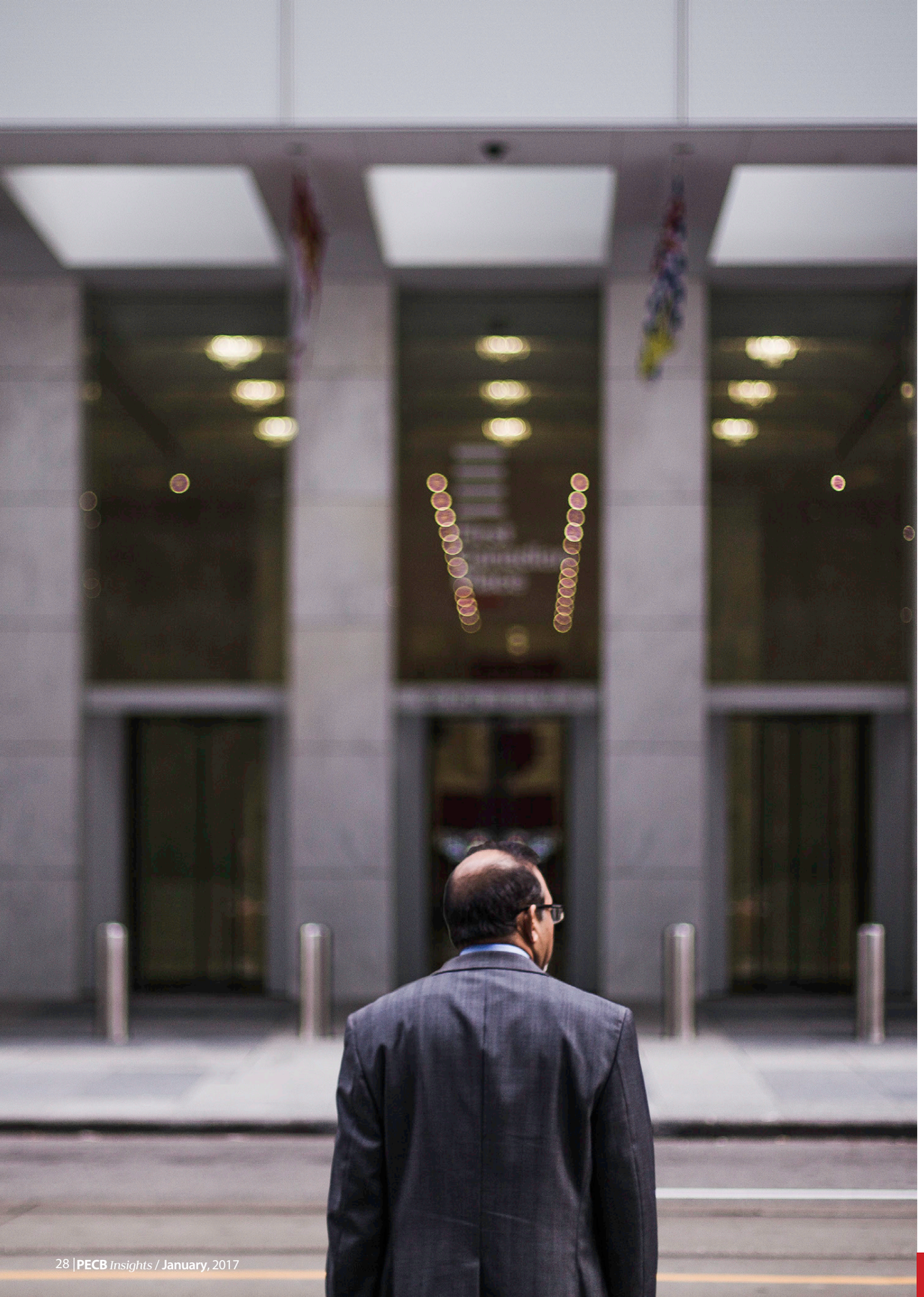
> The PECB Standards Insights Conference will progress in both English and French.

Further, Governance Risk and Compliance management systems get developed to improve operational efficiency and effectiveness to your organizations. This tracks program is developed to maximize the understanding of improving business performance and support transparency, cost control, risk measurement and resilience. Strongly highlighting an organizational culture concentrated in ethics and integrity, Governance Risk and Compliance frameworks also aid to fast and accurate decision making.

As an outstanding sharing experience, PECB is striving to connect their global network of partners and interested parties towards an extensive exploitation of business opportunities in various industries.

Networking through the PECB Standards Insights Conference adds up to the astounding lineup of speakers and influencers, while aiming towards constructive conclusions with respect to our overwhelming panel discussions. This first round is organized by PECB, responsible also to drive the excitement of continuing the journey of providing great quality of education.

Pleasantly, your involvement will indeed amplify our belief to elevate your professional opinions about management systems and their importance to the facilitation of global development, and quality of life.



ORGANIZATIONAL RESILIENCE
FAD OR FUTURE?

Why care for something like organizational resilience? We've got a lot of management and corporate governance tools; we've got a dozen or so ISO system management standards; and on top of that there are a lot of frameworks at our disposal, helping us to better manage an organization.

One might argue about the root causes that a need to "create" something like "organizational resilience" arose from the fact that business continuity management did not provide enough protection for each and every threat to an organization. BCM is certainly the holistic discipline to prepare an organization against the impacts of sudden and large-scale events. ISO technical committee 292 (ISO/TC 292), which has developed ISO 22301:2012, the world's first standard specifying a business continuity management system (BCMS), came up with the proposal to enhance this approach and to establish an overarching approach: describing what it would take to expand on the idea of BCM and to increase the protection envelope.

Yet, it can be observed that most organizations already try to achieve a certain degree of organizational resilience in their own interest, but it is also clear that this approach can be enhanced and put on a more systematic basis. This is one of the main objectives of ISO 22316. As there was no usable definition of organizational resilience, the subject matter has now been defined as: "ability of an organization to absorb and adapt in a changing environment".

Similar to business continuity, we are talking about a changing environment, but the changes are no longer just short-term catastrophic effects, such as power outages, floods, or cyber-attacks, but the environment may change rather slowly, maybe even on a non-noticeable scale on a day-to-day basis. But, still these gradual changes may bring down an organization in the long-term. For example, if an organization is failing to adapt to changes in customer requirements or taste, it will have problems in the future. If an organization ignores changes in legislature, currency exchange rates, rising political instability, etc., this organization may not feel any impact next week or next month, but might arrive to be in a very uncomfortable position a couple of years down the road. Frankly, this multi-dimensional challenge of managing and adapting to a changing environment appears to be a core ability of organizational resilience.

In ISO 22316, a three-pronged, structured approach involving principles, attributes, and activities is proposed. *Principles* provide a foundation for enhancing an organization's resilience; *attributes* describe the characteristics of an organization that allow the principles to be adopted. Finally, *activities* guide the utilization, evaluation and enhancement of attributes.

First of all, as a foundation, organizations need to adhere to certain *principles*, without which a gradual development of organizational resilience seems to be futile. As a consequence, organizations need to follow a range of principles in order to

have a chance to work towards organizational resilience.

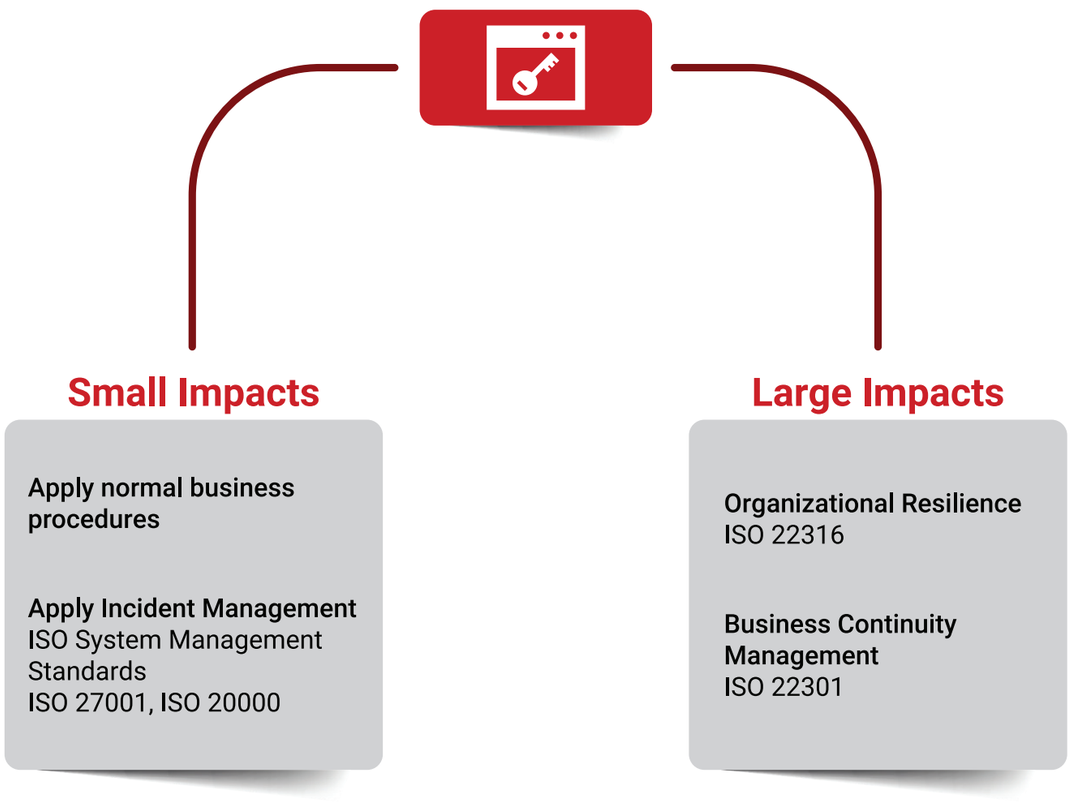
Secondly, organizations need to display certain *attributes* contributing to organizational resilience; they need to adopt these attributes. Finally, observing the principles and displaying the attributes, a range of *activities* need to take place. The common goal of these activities is to guide to the evaluation and enhancement of attributes. So we are not asking for a kind of passive properties such as possessing principles and displaying attributes, but the approach to organizational resilience consists of performing a range of favorable activities.

Consequently, because of space limitations, let us just have a look at selected examples of principles, attributes and activities.

Examples of a favorable principle are behaviors of all members of the organization in order to contribute to organizational resilience. Passive or counter-productive behavior should be avoided. This also means that the workforce should consist of resilient people itself, in order to building resilience from the bottom up. If there is non-engagement within the workforce, a high degree of absenteeism, or if the workforce is kind of fighting against management, we see behaviors not contributing to organizational resilience;

An example of what a favorable *attribute possesses is an understanding of the context of the organization*. This is a very important attribute which again contributes to enhancing the organization, not only as part of managing risk, but also in order to identify opportunities. These opportunities may range from being more immune to changes in the political landscape to innovative product ideas;

Another example for a very important *activity* to enhance organizational resilience is the establishment of a culture of continual improvement. Of course, this approach is not unique to organizational resilience: striving to improve is part of every ISO systems management standard such as ISO 9001, ISO 27001, ISO 22301, etc.



Finally, ISO 22316 cites examples of management disciplines which need to be implemented at a high maturity level and which need to synergistically enhance each other in order to contribute to organizational resilience. Depending on the industry of the organization, some of these management disciplines might be more important than other ones. However, it can safely be assumed that such management disciplines like business continuity management, environmental management, financial control, information security management, quality management and risk management need to be established and support each other.

So, what are critical success factors contributing to organizational resilience? We certainly need a holistic and interdisciplinary approach, as organizational resilience is not a departmental responsibility, but is the responsibility of the whole organization. This starts with full management commitment (from the top) but needs to spread out to all staff of the organization: if nobody knew where the organization is heading and how to make it more resilient, management would be powerless. Organizational resilience also needs a 360° monitoring in several areas, such as legal, compliance, politics, competition, environment, market and consumer trends, foreign exchange, and others.

As organizational resilience is a young discipline, ISO 22316 is not a specification standard (you cannot as an organization be certified against it), but it provides valuable guidance on what an organization needs to undertake to progress on the path to organizational resilience.

PECB

Integrating resilience in your organization does not only bind to supporting sustainable development of your organization, but also initiates a quality culture within the working environment. Therefore, training against ISO 22316 through PECB will give your organization the advantage of pursuing a resilient organizational culture while having the ability of fast response to unexpected changes. The advantage of training on Organization Resilience will also be prone to elevate the performance of your employees in terms of both skills and attitudes of supporting fast changes.

ABOUT THE AUTHOR

Mr. Wolfgang Mahr has been the Owner and Managing Director of Governance and Continuuuity from January 2010 to present. As a Business Continuity Management expert, and IT Governance specialist, he has also participated in the development of ISO 22301, ISO 22313, and ISO 22317, as the head Swiss Delegation. Moreover, his specialties have been passed onto other professionals through his years of lecturing Information Security at ABB Technikerschule. His experience has also found room to consult various organizations through his experience at BNI Axept AG, Ultraflex AG, and Intercai AG. Additionally, Mr. Mahr has numerous projects with Siemens, and The Swiss-South African Co-Operation Initiative, and as an Owner and Managing Director at Fairhills Academy cc.

REMAINING SAFE AND SANE AT WORK

Many organizations have continued to see the growing need for ongoing implementation of safety within the workplace. In 1999, BSI (British Institute of Standards) released the OHSAS 18001 standard, the Occupational Health and Safety Management System. This standard was put into place on a global level, and has continued to grow with the 2007 revision. Currently, ISO 45001 has been created to succeed OHSAS 18001:2007, and although it is lined up with other standards such as the ISO 9001 and ISO 14001:2015 editions, the 2016 release has currently been delayed until 2017.

Why do we need to have a safe workplace environment and what impact does it have on employee performance? Many, to be blunt! Developed countries have the need to keep employee injuries to a minimum at a financial level. Higher injury rates, equals more money spent on medical costs, lost time, etc. In those countries where worker's rights are not as highly regarded or regulated as in developed countries, safety standards such as OHSAS 18001 or the upcoming ISO 45001, assist in filling that gap in local legislation to ensure that employee safety is the main goal and actions of the organization speak to that goal.

Nonetheless, employee productivity is not increased by being lucky or having nice workers. It is a very specific outcome that can be molded through safe practices. On that note, less down time, increased working rates, and healthier workers are all usually positive drivers in maintaining or increasing production numbers.

Think about it as though you are driving a car down the road. If it is a nice sunny day, and the speed limit is 50, you as the driver can safely and easily go this speed. Think of a sunny day as normal production. Now, say that you are driving at night time or in the rain, what safety measures would you need to keep your same constant rate of speed of 50? Clearly, headlights, windshield wipers, etc. Without these tools, you would not maintain or want to increase your speed without a greater potential of an accident occurring. The same can be said for having safety in place within your organization. If that safety is through engineering controls, you might have guarding for machinery, whip checks for high pressure lines, sound barriers to ensure that normal conversations could take place without shouting, etc.

Now, we just covered one hierarchy of safety, engineering controls. The same example/ exercise could be utilized for eliminating hazards, substitution for hazards, putting administrative controls in place, or lastly simply implementing the use of safety equipment or PPE.

Moreover, all of these steps should be in place within an organization through appropriate and documented procedures, policies, work instructions, standard operating procedures, etc. Without a firm structure that can be followed, and understood by every employee, safety cannot remain resilient and continually be improved and strengthened. This in itself can be challenging. Many, many organizations may be doing the right thing, and injuries seem to be at acceptable levels; but very often the trend is that without this support and structure, a few small incidents can continue to snowball and grow into an uncontrollable safety issue.

Has top management been a key supporter and leader of safety? Are there steps in place to look at and assess each task, job duty, machinery that is utilized, to ensure that proper safety applications have been put into place? Are potential issues or hazards thought of, through risk analysis? All of these should be looked at through internal reviews and/or audits of the organization. Yet, there should be materials that are easily reviewed that are put into place to ensure that a safe work environment is being maintained.

When reviewing one's safe practices, it is also key, to ensure that they are in compliance and line up with local legislation; on a national, provincial, state, county, city, or other level. In the US, it is easy to spot the usual suspects. In fact, OHSA does a great job of summarizing and reporting the top 10 "serious" violations each year. For a quick example, the list for 2015 included: fall protection, scaffolding, hazard communication, LOTO, ladders, respiratory protection, machine guarding, powered industrial trucks, electrical – wiring methods, and electrical – general requirements. These actually line up fairly well with what we at JT Environmental Consulting see with clients, on a global level. Unfortunately, many of these are important aspects to review with new employees upon hire, and not implementing this important training can lead to accidents and potential fines.

Ultimately, having a safe work environment takes a lot of effort, and ongoing work. It can only be as good as the employees, visitors, and contractors that participate. So having a more robust and easy to follow program seems to be the key to most leading safe organizations. Having this foundation also provides an easy stepping stone for ensuring that an organization is ready to meet the needs to gain and/or maintain certification to current standards such as OHSAS 18001, and future standards such as ISO 45001.

PECB

The priority put in terms of Health and Safety at work is tightly linked to not only a friendly working environment, but is also directly affecting employee productivity. Maintaining a safe workplace should be continuously scrutinized as much as improved towards an ergonomic setting. Offering training to implement and maintain such an environment, PECB may also certify you against OHSAS 18001, while ensuring your commitment to employees' wellbeing.

ABOUT THE AUTHOR

Jason Telizcak is currently the CEO of JT Environmental Consulting Inc. from where he has practiced counseling in a variety of industries including, Auditing, Data Security, Energy, Environment, Engineering, e-Waste, Food Safety, and Green Construction among others. His engineering experience has been also employed at Jacobs as a contracted Project Management Engineer. Further, Mr. Telizcak has been active at Edwards & Kelcey Engineering, Elmhurst Chicago Stone, and Elk Grove Park District.

AUTHOR OF THE MONTH

Harvey Berger

Is a highly seasoned CPA, and risk based professional. Harvey has over twenty-five years' experience in aligning information security to business process improvement. He has assisted small and Fortune 500 companies in the prevention, detection, and recovery from security breaches. As a team leader, he received praise and awards for Cybersecurity assessments, and for security architecture redesigns. This includes two of the largest security fraud restructuring engagements in USA history.

Harvey has managed numerous internal and external audits on high risk complex computer systems. He has performed special internal audit quality reviews including anti-money laundering compliance for major international banks. In addition, Harvey was also quoted as an SAP expert in "How to Survive an SAP Audit", SAP Press 2010 and also taught Institute of Internal Auditors SAP Implementation and Process Auditing.

Harvey has formerly held government security clearance, and is a certified PECB instructor for teaching ISO Standards, CPA (USA) Accounting Review Courses, and the CISA Preparation Course. He has and is also a frequent speaker on security, design assessment of controls, cybersecurity, fraud awareness, and process improvement.

Harvey Berger

LEGAL DOCUMENTS AND STATE PROPERTY PROTECTION

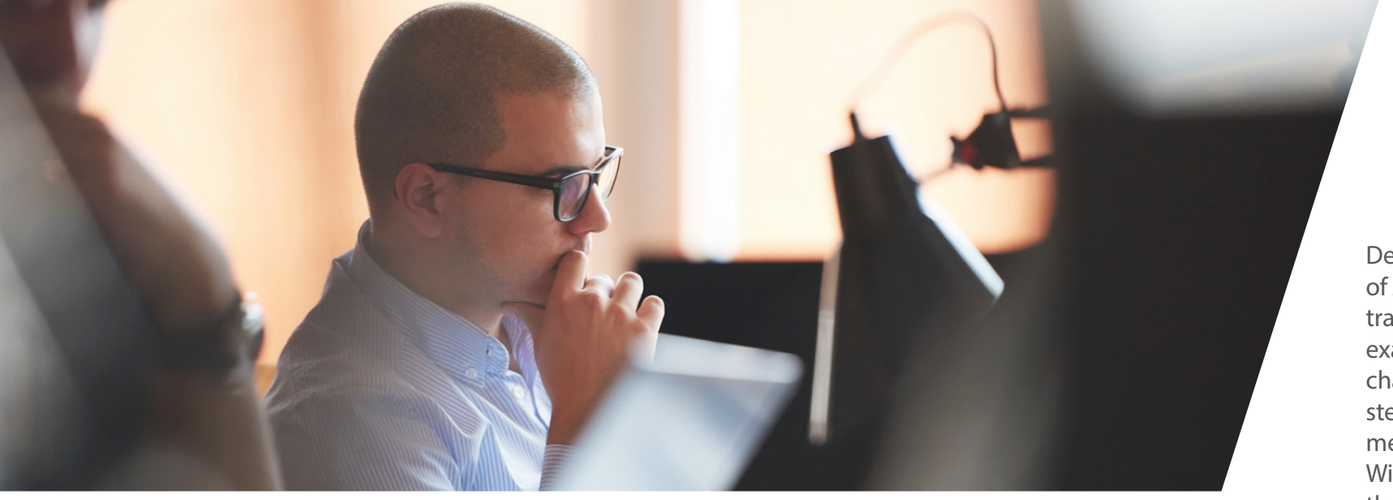
A STRATEGIC APPROACH

In 2016, data breaches remain one of the most significant challenges facing law firms and government agencies. Cybercriminals target law firms and government agencies due to the value of the intellectual property and sensitive information that they maintain.

Since 2013, for the industries being tracked, approximately five (5) billion data records have been reported as either lost or stolen. Of this amount, over 14% of breaches were government related. The reality, however, is likely much higher since the Breach Level Index only tracks publicly disclosed breaches. Unfortunately, law firms are not tracked since this information is not public.

In assessing the impact and likelihood of the related risks, people are considered the wild card due to their unpredictable behavior in complying with security policies. They are the weakest link in security compliance, and pose one of the most difficult challenges faced by cybersecurity professionals and easiest target of hackers. The **malicious employee**, whether motivated by money, hatred, or both, is one of the most difficult challenges faced by cybersecurity professionals.

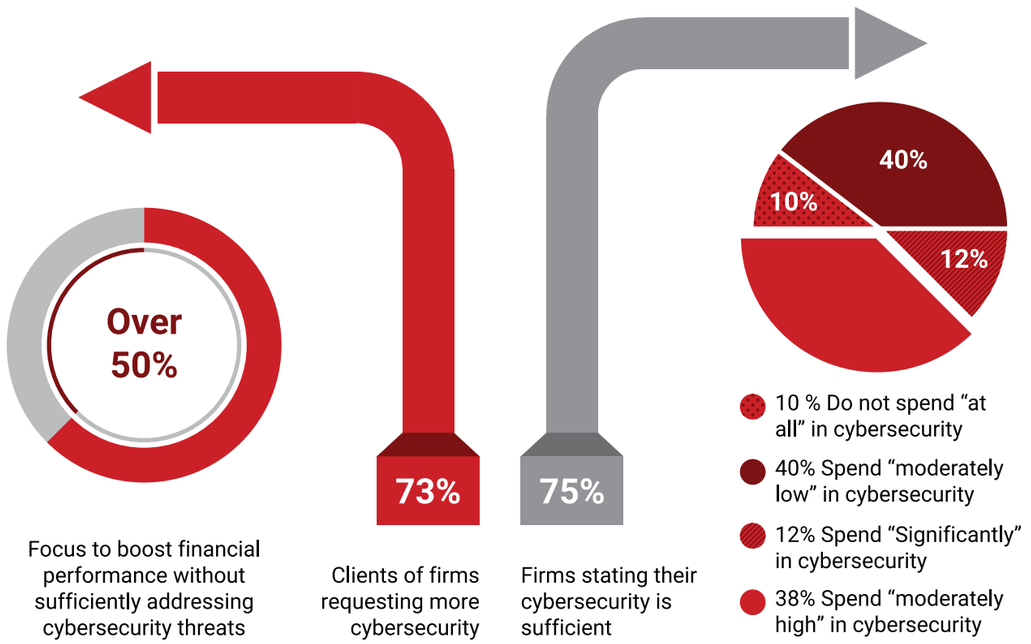
Evidently, a technical cyber solution can be implemented, such as a security information and event management (SIEM) process. However, without sufficient training, incidents can occur and not be detected on a timely basis. One survey cited that on average, it takes 206 days to detect a cybersecurity event and respond. People must know how to detect and respond to cybersecurity incidents on a timely basis.



Although cyberattacks continue to grow, in 2016, law firms have not placed a major business priority on managing cybersecurity. This is alarming since the significant financial and reputational damage resulting from a hack can impact law firms, client-attorney relationships, political and judicial systems.

A recent survey of law firms and legal professionals cited that over 50% of the 800 law firms surveyed stated that they were continuously focused on bolstering their financial bottom line and operations without sufficiently addressing cybersecurity threats. In fact, law firms continue to lag behind in funding their cybersecurity programs. The survey found that 10 % of firms did not spend any of their budget on cybersecurity, while 40 % described their cybersecurity budget as "moderate" compared to 12 % describing their cybersecurity investment as "significant".

The survey also revealed that despite 73% of firms receiving demands from clients to boost their cybersecurity, over 75 % of law firms are confident that their cybersecurity procedures are sufficient. Fact is that most failed to create and test a cybersecurity incident response plan, or have an unqualified audit opinion on security, or do not have security certification by a professional accredited certification body such as PECB.



Despite the survey, recently the USA Department of Justice (DOJ) mentioned instances of insider trading based on hacking of law firms. One example is that three Chinese hackers have been charged in the USA with insider trading after stealing confidential trade information on proposed mergers and acquisitions from American law firms. With this information, the group bought shares in the target businesses and made approximately $4 million in illegal profits.

Governments are moving in the right direction. Recently, New York State proposed a regulation effective March 1st, 2017, stating that financial institutions must establish a program capable of ensuring the confidentiality and integrity of its information systems. This is a complementary to the existing U.S. Government requirement, which states that all federal agencies must develop and adhere to cybersecurity policies and practices which address the following minimum requirements.

Starting with, identifying internal and external cyber risks as well as using a defensive infrastructure is marked as an initial requirement. Additionally, organizations are required to implement a cyber security policy to protect nonpublic information from unauthorized access. Also, they will need to detect and respond to cybersecurity events while ensuring resumption of normal operations following such events. Further, developing written procedures to assess and test the security of externally developed applications is yet another prerequisite; followed by establishing risk-based policies, procedures and controls to monitor activity of authorized users and detect unauthorized access. A timely destruction of personal data lines up here as well. Competent staff and the employment of a CISO (Chief Information Security Officer) to implement and control cybersecurity policies is a requirement.

To provide an in-depth defense, ISO\IEC frameworks can be used as a tool to identify vulnerabilities, and threats using a risk based approach. Cybersecurity controls have been defined and can be utilized. The ISO\IEC frameworks emphasize that cybersecurity is a business risk and not just an IT risk.

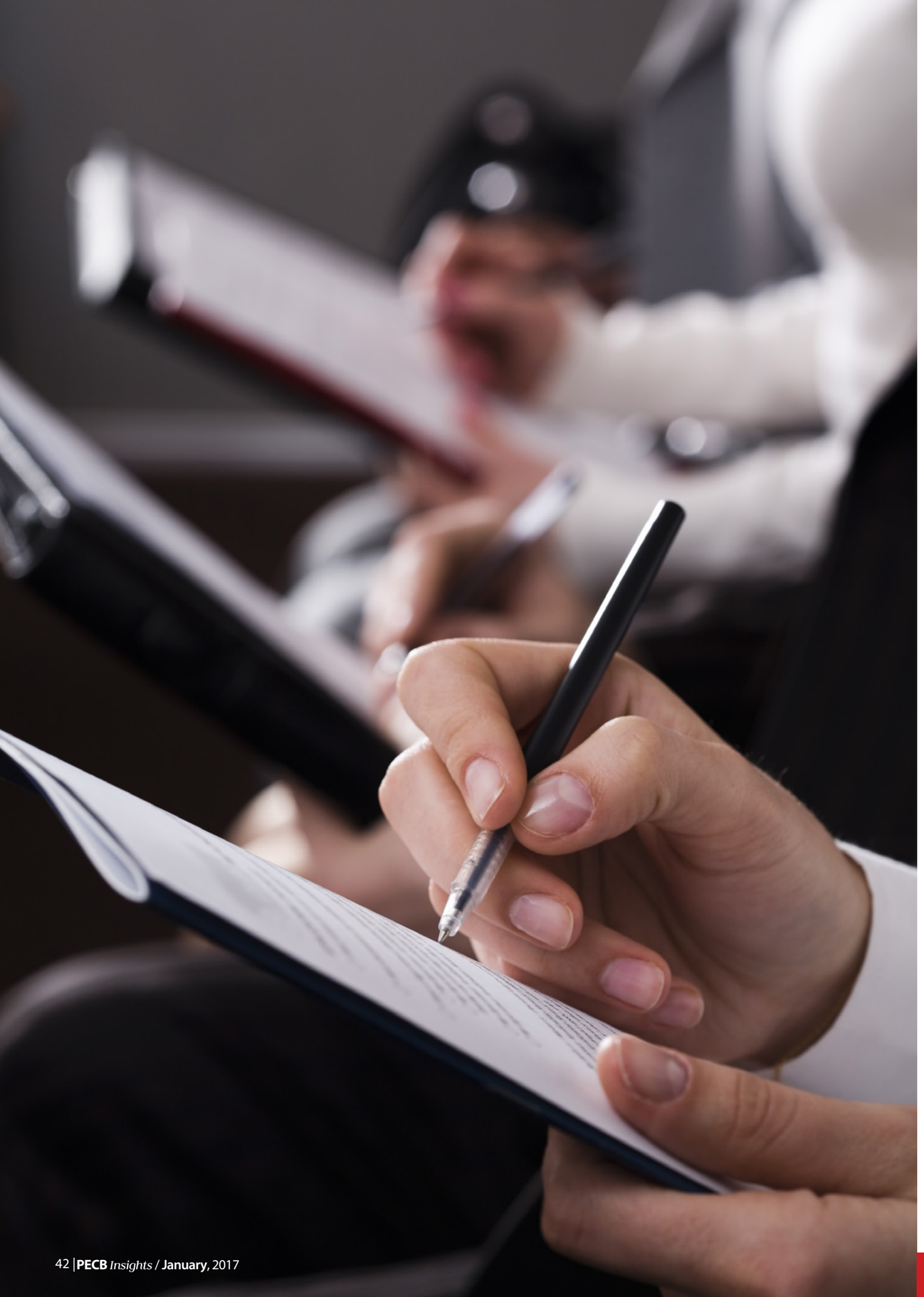
In summary, the need for an effective cybersecurity strategy continues to be important in order to achieve success. ISO\IEC frameworks are here and can help.

PECB

Complying with cybersecurity policies will not only continue to be a necessity at the state level, but will also benefit the organization and protect their network and Information Security. Thus implementing ISO/IEC frameworks; relevant to cybersecurity will greatly aid organizations to achieve such prerequisites. As a global provider of training, examination, audit, and certification services, PECB offers its expertise in multiple fields, including ISO/IEC 27000's training courses.

ABOUT THE AUTHOR

Harvey Berger, CPA, CISSP, CISA, CFE, PMP, CAMS, MCSE, CGMA, CSSBB, ISO-27001 Security Master, ISO 27032, ISO 13053 is a highly seasoned CPA-risk management professional. Harvey has over twenty years of aligning Information Security to Business Process, and has assisted Fortune 500 companies to prevent, detect, and recover from security breaches. He was a team leader for numerous cybersecurity architecture designs. Harvey is a certified PECB Instructor for teaching PECB courses based on ISO Standards, CPA (USA) Accounting Review Course, and for the CISA Review Course. Harvey is also a frequent speaker on security, design assessment of controls, cybersecurity, fraud awareness, and process improvement.



THE VALUE OF KNOWLEDGE ACQUISITION THROUGH TRAINING

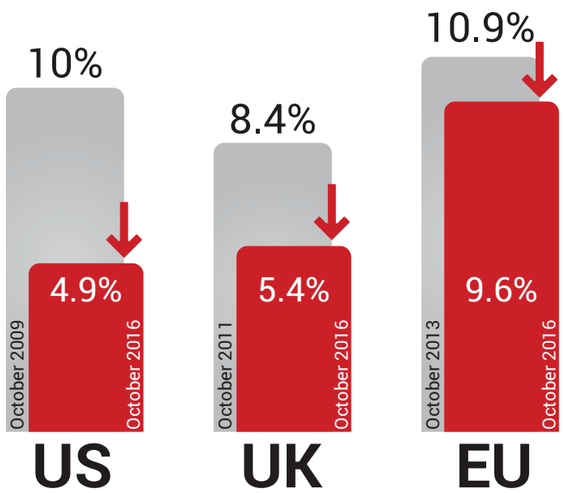
Much has been written about the value of training and certification. Associations tout certification as a means for an individual to demonstrate their knowledge, confirmed by an objective 3rd party, while training organizations boast at their ability in teaching individuals on how to pass certification exams. Undoubtedly, this is partially the case for both, but there is much more to it than a piece of paper and increasing one's probability of getting that paper.

Furthermore, organizations are continuously emphasizing upon knowledge acquisition and attraction of talent. This is merely happening due to the increasing level of complexity in terms of organizational structure and complexity of operations. However, witnessing such knowledge and technical abilities to perform complex tasks competently, is bound to witnessing these specific tasks through training and certification. Also, training and certification is showing to have an effect on increasing the productivity and efficiency of individuals when performing their jobs.

The value of training and certification is also increased, as it is nowadays a requirement for a variety of technically skilled professions.
With that being said, certification is giving employees a competitive edge on the competitive global market of professionals.

While having more competences on paper, employees are increasing their credibility to perform tasks. Besides, they are raising the organizations level of competence to provide services or products that are developed by knowledgeable staff. Another reason for taking advantage of certification and knowledge gained through it is not just self-development, but is also linked closely to finding employment. Employers on the other hand, do take seriously certification when it comes to employment as it presents a substantial effort to take one step further on developing their abilities to perform tasks more effectively and knowledgeably.

According to the US Bureau of Labor Statistics, the US unemployment rate has been in a slow steady decline since hitting a peak in October 2009 at 10% and currently resting at 4.9%. In the UK, the rate has declined to 5.4% from its October 2011 peak from 8.4% while the EU has declined to 9.6% from 10.9% peak in Q2 2013 (source: Eurostat).



So what does this mean for those who are either currently employed, seeking employment or even are employers as well? Undoubtedly, competition for limited available positions in the market is extremely intense, where years of experience, coupled with strong best practice knowledge are highly sought out by employers. For the experienced professional, employers must ensure to stay relevant and up-to-date with the latest practices, techniques, and technologies. For those lacking the experience, it is critical to building on a solid theoretical foundation that incorporates realistic scenarios to be applied to their day-to-day activities while minimizing errors and accelerating their professional growth.

In a recent HireRight survey, 65% of businesses are making investments to improve their ability to find quality job candidates, while 53% find retaining top talent is a challenge. Furthermore, employers continue to demand more from their employees while changing market conditions demand that employees remain abreast with the latest skills, techniques, and knowledge. This can be achieved through the appropriate training and mentorship.

Bottom line, employees must keep their skill levels current and adaptable to remain competitive and to ensure the employers have the highest quality staff; must develop competitive retention strategies which include keeping employee skill levels not only up-to-date but with an eye to the future ensuring the employee has greater job satisfaction, and the employer a higher level of key personnel retention.

PECB

Underlining the value of training and certification, PECB offers training in a wide range of international standards. PECB's expertise includes Information Security, IT, Business Continuity, Service Management, Quality Management Systems, Risk & Management, Health, Safety, and Environment. Showing commitment and competence while elevating organizational performance, PECB ensures to provide you with effective training and globally recognized certification to the benefit of your organization. In addition this will certainly contribute to the overall unemployment decrease.

ABOUT THE AUTHOR

Alex Arvanitidis

With over 20 years of domestic and international experience, Alex is a dynamic and innovative executive, a reputable leader, strategic developer and a masterful tactician for start-up development. His specialties highlight best practices in Business Development, Strategy, Public Relations, Market and Competitive Intelligence, Marketing, and Operational Resilience. Having directing positions, Mr. Arvanitidis has contributed his mastery at "ContinuityLink", "Vizionera Inc.", "ITPG", "netASPx"", "Corpora Software, Inc.", "George Washington University", and "Infor Global Solutions". Further, his contribution is marked at, Invensys (now Schneider Electric), Commercial Ware, Baan and Thomson Holidays.

SPECIAL THANKS TO

OUR PLATINUM PARTNERS

Sedika TECHNOLOGIES

ALTIRIAN Security in Serenity

parker SOLUTIONS GROUP

MOULIK

ContinuityLink

Digital Jewels information value chain consultants

IMACERT

Tecnofor

PECB AUTHORIZED PARTNER PECB PLATINUM PARTNER

OUR GOLDEN PARTNERS

BIT Business and Information Technology

Gennesaret Resources

NUM & ERIC NUMERIC TECHNOLOGIES LIMITED

neam IT-Services GmbH

GREAT LEARNING EDUCATION CENTRE

behaviour

SECURCERT

business as usual

SECURASTAR ISO 27001 EXPERTS

protiviti

alc

BSI

PECB AUTHORIZED PARTNER PECB GOLD PARTNER

GET A GLIMPSE OF THE LATEST CHANGES AT PECB

JANUARY 2017

Following our strong belief in integrity and fairness, PECB is thrilled to keep you updated with the latest changes among the courses it offers. Lining up parallel to your convenience, PECB will continuously inform you of any new course offerings, and translated materials. With a wide network of partners worldwide, we aim to provide you with distinctive and personalized materials while ensuring an as clear as possible understanding throughout the whole course of learning.

Persistent to a continuous improvement culture, our staff has not only shown competence to support superior quality of education, but is also prone to comply with our noteworthy resilience. Certifying to and partnering with PECB ascertains you to exceptionally comprehensive material, besides the professional evaluation and impartiality.

UPDATED COURSES

PECB Certified ISO 13485 Lead Auditor
Now updated conform to the latest version of the standard ISO 13485: 2016.

TRANSLATED COURSES

Advanced Auditing Techniques
From now on, you may find this course translated to Spanish.

PECB Certified 22301 Lead Implementer
From hereinafter, this course is also accessible in German.

PECB Certified ISO 27001 Lead Implementer
Now translated to Brazilian Portuguese.

PECB Certified ISO 31000 Risk Manager
Also translated to Brazilian Portuguese.

More than happy to discuss any questions, suggestions, or concerns, we shall remain in contact through customer@pecb.com or visit us at www.pecb.com

When Standards Matter...