People, Process, Technology

The three key elements for a successful information security system

bsi.

...making excellence a habit.™

Last year witnessed the highest number of information security breaches on record. In their January 2015 report, the Ponemon Institute, an independent research organization, dubbed 2014 as the "Year of the Mega Breach." This year portends to be even more costly to businesses of all sizes. The report states, "2015 is predicted to be as bad or worse as more sensitive and confidential information and transactions are moved to the digital space and become vulnerable to attack."[i]

Organizations are starting to recognize the serious threat cyberattacks can pose and are devoting additional resources developing and improving their information security strategy. Frequently, however, many businesses are relying too heavily on technology and essentially are ignoring the "people and process" components required in a strong information security strategy.

A review of two major breaches in the United States shows just how important these two components are. Anthem Healthcare, a major health insurance company, suffered a massive data breach exposing the personal information of 80 million customers and former employees. Anthem believes the attack began with phishing emails sent to a handful of its employees. According to the February 10, 2015 issue of the Insurance Journal, "Investigators now believe the hackers somehow compromised the credentials of five different tech workers, possibly through some kind of "phishing" scheme that could have tricked a worker into unknowingly revealing a password or downloading malicious software.[ii]

The second massive breach at Blue Cross Blue Shield of Michigan (BCBSM) demonstrated the importance of properly vetting employees and limiting access to sensitive information. According to the Detroit Free Press, an identity theft ring involving an employee of BCBSM stole the personal information of more than 5,000 BSBSM subscribers and used the information to open fake credit cards across the country.[iii]

Analyses of the root causes of these and other recent security breaches show that efforts to protect an organization using solutions based solely on technology do not achieve the organization's objectives of cybersecurity, nor are they viable over the long term. One of the most common reasons for their security programs' failing is the lack of attention given to the organization's overall culture. It is important for organizations to use a strategy that focuses on developing critical competencies, along with solid, consistent, well-managed processes woven throughout the culture of the enterprise. This will result in a more effective and sustainable information security architecture.

How does the law define "People, Process & Technology"?

TAKE NOTICE that the Attorney General deems the documents and information requested by this Subpoena to be relevant and material to an investigation and inquiry undertaken in the public interest.

"Custodian" means any Person or Entity that, as of the date of this Subpoena, maintained, possessed, or otherwise kept or controlled such Document.

"Document" is used herein in the broadest sense of the term and means all records and other tangible media of expression of whatever nature however and wherever created, produced or stored (manually, mechanically, electronically or otherwise), including without limitation all versions whether draft or final, all annotated or nonconforming or other copies, electronic mail ("e-mail"), instant messages, text messages, Blackberry or other wireless device messages, voicemail, calendars, date books, appointment books, diaries, books, papers, files, notes, confirmations, accounts statements, correspondence, memoranda, reports, records, journals, registers, analyses, plans, manuals, policies, telegrams, faxes, telexes, wires, telephone logs, telephone messages, message slips, minutes, notes or records or transcriptions of conversations or Communications or meetings, tape recordings, videotapes, disks, and other electronic media, microfilm, microfiche, storage devices, press releases, contracts, agreements, notices and summaries. Any non-identical version of a Document constitutes a separate Document within this definition, including without limitation drafts or copies bearing any notation, edit, comment, marginalia, underscoring, highlighting, marking, or any other alteration of any kind resulting in any difference between two or more otherwise identical Documents. In the case of Documents bearing any notation or other marking made by highlighting ink, the term Document means the original version bearing the highlighting ink, which original must be produced as opposed to any copy thereof.

"Sent" or "received" as used herein means, in addition to their usual meanings, the transmittal or reception of a Document by physical, electronic or other delivery, whether by direct or indirect means.

~**Excerpts from a subpoena**~ (State of New York, 2013)

This is an example from a subpoena issued by the Attorney General of New York. Note that 'People" is defined as a custodian, *"Person or Entity that, as of the date of this Subpoena, maintained, possessed, or otherwise kept or controlled such Document"*. The "Process" in this case is defined as the creation of documents and describes *"all records and other tangible media of expression of whatever nature however and wherever created, produced or stored (manually, mechanically, electronically or otherwise), including without limitation all versions whether draft or final…."*, and "Technology" described as *"Sent" or "received" as used herein means, in addition to their usual meanings, the transmittal or reception of a document by physical, electronic or other delivery, whether by direct or indirect means*. While each case is different, the types of information that can be up for discovery and how *People, Process* and *Technology* are defined can be very broad in the eyes of the law. If an organization does not have an enterprise management system that entails adequate Governance, Risk and Compliance (GRC), as outlined in Figure 1, meeting the requirements of the law could be an expensive and daunting task.

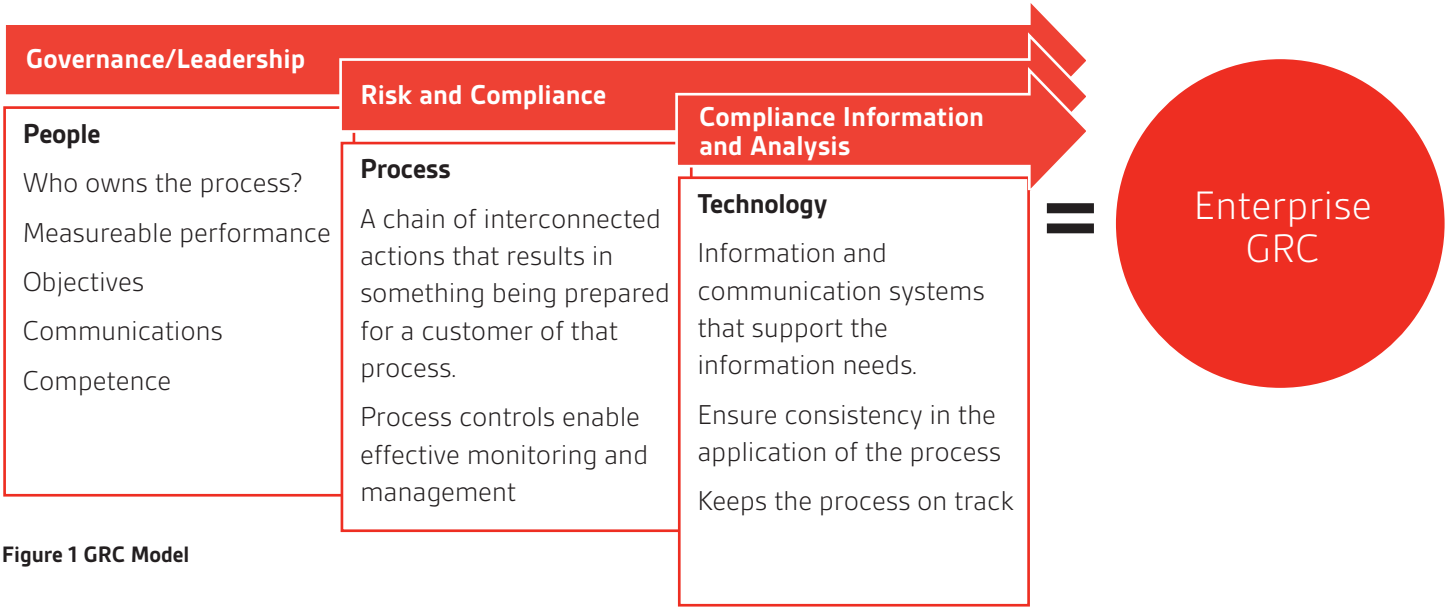


Figure 1 GRC Model

Technology

Often teams instituting change devote most of their efforts implementing technology-based solutions to secure their organization and data, building a "hard shell" around the external walls. While technology-related, most breaches start internally through vulnerabilities associated with people and processes. Organizations that are hard on the outside but soft on the inside follow this "egg shell" security model.

Very often, organizations allocate resources and money on technology to solve business challenges, only to find that the new technology exacerbates the problem. A technology-first mentality frequently provides only a temporary fix, if any.

"Egg Shell" security model

Outer Shell

Firewalls, Filtering Routers, User Names, Passwords, Segmentation, Compartmentalization

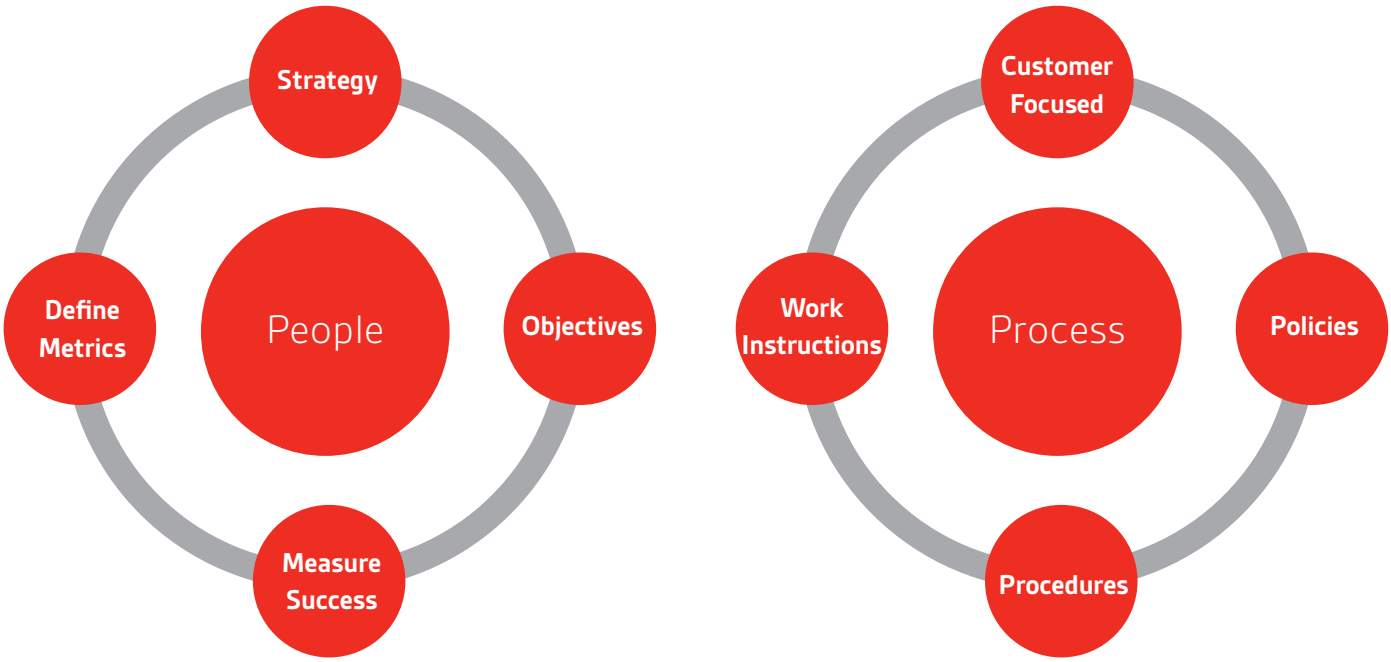
Soft in the Center

Example Technical Structure Diagram

E-mail, instant messages, books, papers, files, notes, confirmations, account statements, correspondence, memorandums, reports, records, journals, registers, analysis, plans, manuals, telegrams, faxes, telexes, wires, telephone logs, telephone messages, message slips, minutes, notes or records or transcriptions of conversations, communications or meetings, tape recordings, video tapes, disks and any other electronic media, Microfilm, microfiche, any storagte devices, press releases, contracts, agreements, calendars, date books, appointment books, diaries, notices.

People and Process

By defining people and process in the business first, an organization can invest in the right technology to make them more effective and provide greater information security. Organizations can then achieve their objectives more effectively and at a lower cost.



The technology subsequently acquired will make both the people and process more effective. It is important that organizations become familiar with how technology integrates with people and processes in order to design an effective, balanced, resilient and well-aligned strategy for information security.

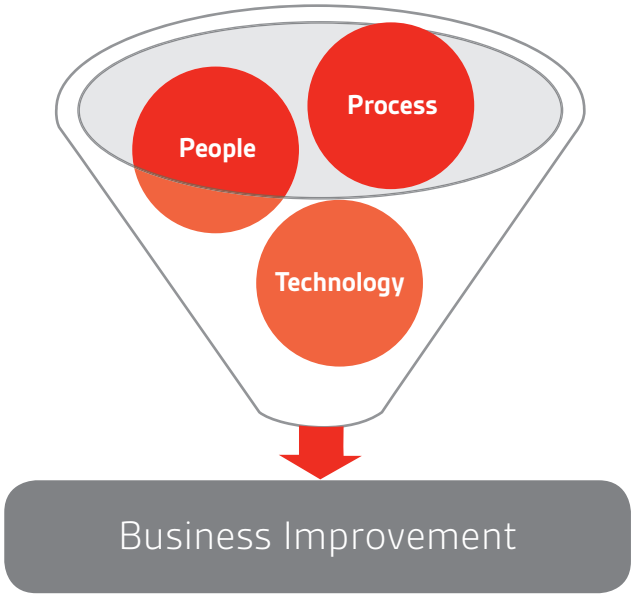


Figure 2 Business Improvement Model

Implement Once, Comply Many

ISO/IEC 27001 is the international standard that describes the specifications for establishing, implementing, maintaining and continually improving an information security management system.

ISO/IEC 27001 applies a risk management approach to securing information and is part of and integrated with the organization's processes and management structure. With its extensive controls, ISO/IEC 27001 helps organizations address the three components of a secure program: people, process and technology.

A holistic approach to information security, ISO/IEC 27001 allows organizations to manage the confidentiality, integrity, and availability of their information assets. Organizations are able to design an "Implement Once, Comply Many" security program, which can aid in protecting, measuring, monitoring, and improving the security across the enterprise and can encompass compliance to the requirements and regulations of a variety of industry-specific security protocols, under one internationally-recognized umbrella.

BSI Solutions

BSI provides a full suite of services including training, assessment and management system software developed to help protect organizations of all sizes. As an Information Security Management System, ISO/IEC 27001 is designed to help you select adequate and well-balanced security controls, which will protect information assets and give confidence to interested parties, including customers, investors and other stakeholders.

Certification to ISO/IEC 27001 is an essential safeguard for any organization. In addition to certification services, BSI offers a range of training courses that are designed to provide the tools needed to understand ISO/IEC 27001, as well as oversee audit programs for an organization's management system. BSI works with this standard, and many more, to protect organizations and their most valued assets from potential threats.

[i] Ponemon Institute Research Report, "2014: A Year of Mega Breaches", page 1. http://info.identityfinder.com/rs/identityfinder2/images/2014TheYearOfTheMegaBreach.pdf?mkt_tok=3RkMMJWWfF9wsRonu6vMZKXonjHpfsX56%2B0sXKOyIMI%2F0ER3fOvrPUfGjI4ATMtrI%2BSLDwEYGJlv6SgFSbbMMa96y7gFXBc%3D, Accessed 4/26/2015

[ii] Brandon Bailey, "Investigators Suspect Anthem Breach Began with 'Phishing' of Employees", 2/10/2015, http://www.insurancejournal.com/news/national/2015/02/10/357051.htm, accessed 4/26/2014.

[iii] Tresa Baldas, "Feds: Identity theft hits Blue Cross Blue Shield" 3/11/2015, http://www.freep.com/story/news/local/michigan/detroit/2015/03/10/identity-theft-blue-cross/24718251/, accessed 4/26/2015.

[iv] State of New York. (2013, October). *SUBPOENA DUCES TECUM - The People of the State of New York.* Retrieved from Electronic Frontier Foundation: https://www.eff.org/files/2013/11/11/exhibit_3._nyag_subpoena_10-4-13.pdf

We know ISO/IEC 27001

BSI shaped the original standard

BSI...

- Shaped the original ISO/IEC 27001 standard
- Has the most highly trained and knowledgeable assessors
- Offers the widest range of support solutions in the marketplace
- Is the number one certification body in the UK, USA amd Korea
- Looks after more that 70,000 global clients
- Has an unrivalled international reputation for excellence

bsi.

bsigroup.com

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA
Tel: 1 800-862-4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
www.bsiamerica.com

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada
Tel: 1 800 862 6752
Fax: 1 416 620 9911
inquiry.canada@bsigroup.com
www.bsigroup.ca
www.bsigroup.ca/fr

BSI/USA/449/MS/515/E