Building a successful company culture often comes down to three elements: people, processes, and technology. The triple-braided cord is strong; but, is interdependent.

A lot of education out there today emphasizes processes and technology; but effective security cannot be achieved without an organization-wide dedication to security.

This is where people come in and the human resources management function can really add value. From top-down to bottom-up, the best security cultures weave all three of these elements together effectively.

Risk management creates value and is an integral part of organizational business processes.

Risk Management is part of decision making; explicitly addresses uncertainty; is systematic, structured and timely; is based on best available information; is tailored; is dynamic, iterative and responsive to change; and facilitates continual improvement and enhancement of the organizational operation.

ISO 31000 is intended to provide guidance on the nature of the risk management process and how to implement it. Companies planning on implementing the COSO ERM framework should review ISO 31000 (and other frameworks) for additional perspective and guidance on implementation considerations.

While some feel that traditional firewalls, antivirus software and intrusion prevention systems (IPS) have lost their usefulness, these security technologies are, in reality, still very much in use -- and needed. However, more robust, effective and, especially, integrated products are often required to keep up with those that threaten today's network infrastructures.

Firewalls have been a first line of defense in network security for over 25 years. A firewall can be hardware, software, or both that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.

A firewall is a network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

The firewall network security device monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

A firewall acts as a barrier between a trusted network and an untrusted network. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied.

Five basic types of firewall protection exist--network level, circuit level, application-level, stateful multilayer and next generation platform.

Each type has advantages and disadvantages, ranging from ease of implementation to high initial cost. Companies should use the firewall as part of an overall information security program that includes data integrity, application integrity and data confidentiality and authentication.

Fundamentally, all data traffic either flows in or out of a computer, and this two-way traffic is controlled using firewall technology. Many organizations have an internal network similar to the internet; however, is called an intranet. Intranet is a TCP/IP network that is modeled after the Internet that only works within the organization. To protect databases, servers, and computers from receiving corrupt data, a firewall is put in place. Furthermore, to protect sensitive data from unauthorized access, a firewall is put in place. Different types of firewalls are implemented to perform specific functions in the protection of data ... with traffic either coming or going within the network.

Using rules defined by the system administrator, the firewall allows data to pass; however, if data does not pass scrutiny, it is disregarded and does not pass. The firewall sits at the gateway of a network or sits at a connection between two networks. All traffic, from one network to the other, passes through the firewall analysis matrix. The firewall stops or allows traffic based on the security policy as defined in rules' table.

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made.

Antivirus (anti-virus) software is a class of program that will prevent, detect and remediate malware infections on individual computing devices and IT systems.

An antivirus is a utility software that searches a hard disk for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.

Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses.

However, antivirus programs are useful for preventing infections caused by many types of malware, including worms, Trojan horses, rootkits, spyware, key-loggers, ransomware and adware.

In marketing, the terms antivirus and antimalware are often used as synonyms.
There are thousands of computer viruses out there today. It is essential that you have an antivirus software installed on your computer to help protect your system. This protection will defend your system against potential damage, as well as protect your personal information from being spread throughout the Internet.

A techno-savvy sub-culture has developed in which code writers develop viral software in the spirit of competition ... and they give their virus a 'name' in hope of gaining fame. Still, others develop malicious code with the intent of wreaking havoc on other computer systems with myriad motives. And of course, some develop spyware to gain confidential information or plant corrupt information. The term 'hacker' seems to carry with it a sense of prestige; however, even with ethical justification, it is unauthorized. The need for effective and evolving data security is paramount in the contemporary techno environment.

Intrusion Prevention System (IPS) is a system that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.

Intrusion prevention systems are basically extensions of intrusion detection systems. The major difference lies in the fact that, unlike intrusion detection systems, intrusion prevention systems are installed are able to actively block or prevent intrusions that are detected. For example, an IPS can drop malicious packets, blocking the traffic an offending IP address, etc.

The IPS often sits directly behind the firewall and it provides a complementary layer of analysis that negatively selects for dangerous content. The IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network and must work efficiently to avoid degrading network performance.

A VPN, short for virtual private network, is a data security service that uses encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. A user's data is kept secure, and internet activity cannot be detected by anonymous or insidious parties collecting such information.

The first step to security is usually a firewall between the client and the host server, requiring the remote user to establish an authenticated connection with the firewall. Encryption works by having all data sent from one computer encrypted in such a way that only the authorized receiving computer can decrypt the data.

This keeps data secure, particularly on public Wi-Fi networks in places like coffee shops and airports, ensuring no one can snoop your traffic and steal your passwords or credit card numbers. Since VPNs route your traffic through another network, you can also make it appear as if it's coming from another location.

Using a VPN is considered as a smart move. Today there are tons of VPN service providers that makes it difficult to choose one. Foreseeing your VPN needs, setting aside some time and looking for quality rather than low-cost can turn out to be critical in ending up with the best VPN Service Provider. Using a VPN can cause the speed of the internet to deteriorate, however, a reputed or efficient VPN service provider can handle and maintain things smooth so that the speed change is subtle. Most organizations rely on VPN security to facilitate remote access for businesses from multiple offices.

In large-scale enterprises the possible combinations of application scenarios and communication media complicate administration and configuration of components. A remote access solution, containing several thousand users, quickly becomes highly complex and quickly drives administration, support, training and documentation costs up.

Along with the evolution of risk management in general has come the need to maintain mechanisms to keep traffic safe from outside intrusions. VPNs provide one of the pieces in this puzzle that offer organizations the ability to maintain a connected workforce, along with high levels of security.

Cyber Security – Part 1

As threats continue to mount, understanding and managing cyber-security risks has become a top priority for leaders in business and government. Organizations are responding by taking action. Increasingly, they are adopting innovative technologies like cloud-enabled cyber-security, Big Data analytics and advanced authentication to reduce cyber-risks and improve cyber-security programs.

Businesses are also embracing a more collaborative approach to cyber-security, one in which intelligence on threats and response tactics is shared with external partners. Internally, organizations are rethinking the roles of key executives and the Board of Directors to help create more resilient and proactive security capabilities.

Another notable measure of progress is a renewed willingness to invest in security. This year, business managers have significantly boosted information security spending to better enable them to tackle the cyber-security juggernaut head on. The threat of hackers and cyber-criminals is very real, for large companies and small businesses alike. And governments continue to realize that their data security is paramount.

Business owners and government agencies must accept that a strong cyber-defense system is a ‘must have’ in the modern business world. The good news is that there are lots of security firms out there willing to add support. But hiring a security services firm doesn’t let business managers off the hook. Just because the work of defending a company’s sensitive data can be outsourced to a third party, doesn’t mean the management accountability is obsolete when information is un-secure, internally as well as externally.

> “Every organization is ultimately responsible for the security of its valuable information; but competent business leaders know when to use reliable third-party systems to augment internal controls and achieve less risk with fewer vulnerabilities to worry about and – perhaps more importantly – to mitigate the potential damage that would be caused by any breach.” – Donald Olson

The rewards of risk-based frameworks ... a risk management function.

The vast majority of organizations have adopted a security framework or, more often, an amalgam of frameworks.

The most frequently followed guidelines are ISO 27001, the US National Institute of Standards and Technology (NIST) Cyber-security Framework and SANS Critical Controls.

Respondents say adoption of these types of guidelines enable them to identify and prioritize threats, quickly detect and mitigate risks, and understand security gaps.

A risk-based framework allows companies to better communicate and collaborate on cyber-security efforts, internally and externally.

These frameworks also can help businesses design, monitor, and measure progress toward goals to achieve an improved cyber-security program. And many say that risk-based standards have helped ensure that sensitive data is more secure in terms of comprehensive objectives and accountability.

Managing cyber-security risk isn't about eliminating all risk. It is about determining and understanding the risk rating of events and putting the right processes or controls in place to manage them in accordance with the organization's risk tolerance levels.

It is an ongoing process, not a one-time event. And it requires an organization to understand what kind of events can have a negative impact on operations, how likely those events are to occur, and what the impact would be to the service or business if a given event does occur.

The framework helps an organization determine a set of cyber-security goals and desired security outcomes, arranged according to **5 functions:**

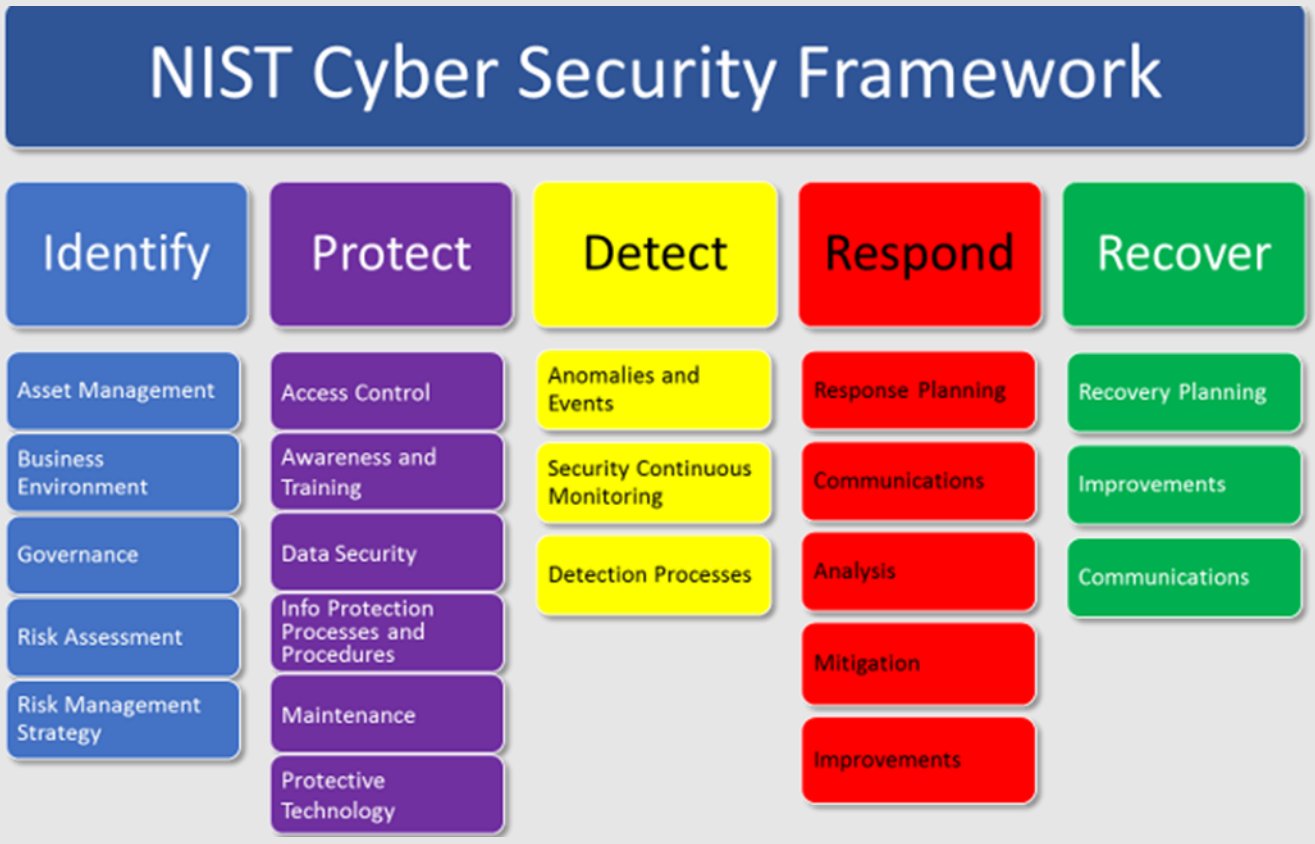
1. **Identify:** Use organizational understanding to minimize risk to systems, assets, data and capabilities.

2. **Protect:** Design safeguards to limit the impact of potential events on critical services and infrastructure.

3. **Detect:** Implement activities to identify the occurrence of a cyber-security event.

4. **Respond:** Take appropriate action after learning of a security event.

5. **Recover:** Plan for resilience and the timely repair of compromised capabilities and services.



Awareness is a key factor that precedes a proactive and effective cyber-security strategy.

Harnessing the power of cloud-enabled cybersecurity

Cloud computing has emerged as a sophisticated cyber-security tool in recent years as providers have steadily invested in advanced technologies for data protection, privacy, network security, and identity and access management.

Many also have added infrastructure capabilities that enable them to improve intelligence gathering and threat modelling, better block attacks and accelerate incident response.

It's no wonder, then, that this tool has become a best practice for business leaders to use cloud-based cyber-security services to help protect sensitive data and ensure privacy.

The CIO and other senior business executives need to take responsibility for bringing their organizations into the era of cloud computing.

I.T. managers entrust a broadening range of critical services to the cloud, including real-time monitoring and analytics, advanced authentication, and identity and access management.

Some people maintain that there's nothing magic about the cloud—that anything it can do, well, on-premise approaches can also accomplish. That argument is correct in theory, at least for large companies that can and will afford comprehensive enterprise software and top IT talent.

Such companies spend vast resources to buy or build software for collaboration or analytics—or anything else—and install it in their own data centers.

They can enable these applications for different devices—desktops, laptops, tablets, and smartphones—and make them accessible to employees at home and on the road via web browsers.

They can also open this infrastructure to people outside the organization, such as contractors, suppliers, and joint venture partners.

Essentially, the cloud service providers have already done this, and client organizations pay a set subscription fee and simply login and start work. This approach is cost effective, controls costs, and gives all members, even smaller organizations, an even playing field.

There is great value in both cloud-based cyber-security and cloud-based operations.

Cloud security, compliance, and the certificates that help support cloud communication have all come a long way. When it comes to compliance and regulatory-driven organizations, it’s important to understand how technologies like cloud and virtualization are now able to create a more robust environment.

Moreover, mobility solutions – when incorporated with the cloud platform – can even further enhance the data center cloud security model. Remember, there are still organizations out there which are heavily driven by compliance requirements such as SOX, HIPAA, PCI/DSS and even FISMA. While not all solutions are the same, many are highly recommended and highly functional.

Typically, you get what you pay for ... So the point is that the acting CIO should develop a list of requirements and then go shopping. Once a list of potential vendors is drafted, the CIO can assess value based on price, performance, additional services, and industry reputation. Government offices often advertise an RFP or ITN.

You might be surprised, as one vendor was willing to pay all upfront implementation costs and create a 'case study' designed as a marketing strategy to earn future business. Success with one client is a vehicle to winning the business of potential clients.

The BIG impact of Big Data

Big Data is getting bigger and introducing new-found intelligence into the managerial decision making process.

Business leaders have learned to leverage Big Data analytics to model and monitor for cyber-security threats, respond to incidents, and audit and review data to understand how it is used, by whom and when.

A data-driven approach can shift cyber-security away from perimeter-based defenses and enable organizations to put real-time information to use in ways that can help predict cyber-security incidents.

Data-driven cyber-security allows companies to better understand anomalous network activity and more quickly identify and respond to cyber-security incidents.

Organizations are exploring the use of data analytics for identity and access management to monitor employee usage patterns, flag outliers and identify improper access.

Some businesses are combining Big Data with existing security information and event management (SIEM) technologies to generate a more extensive view of network activity.

Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization’s information technology (IT) security.

The acronym is pronounced "sim" with a silent e.

SIEM systems are typically expensive to deploy and complex to operate and manage. While Payment Card Industry Data Security Standard (PCI DSS) compliance has traditionally driven SIEM adoption in large enterprises, concerns over advanced persistent threats (APTs) have led smaller organizations to look at the benefits a SIEM managed security service provider (MSSP) can offer.

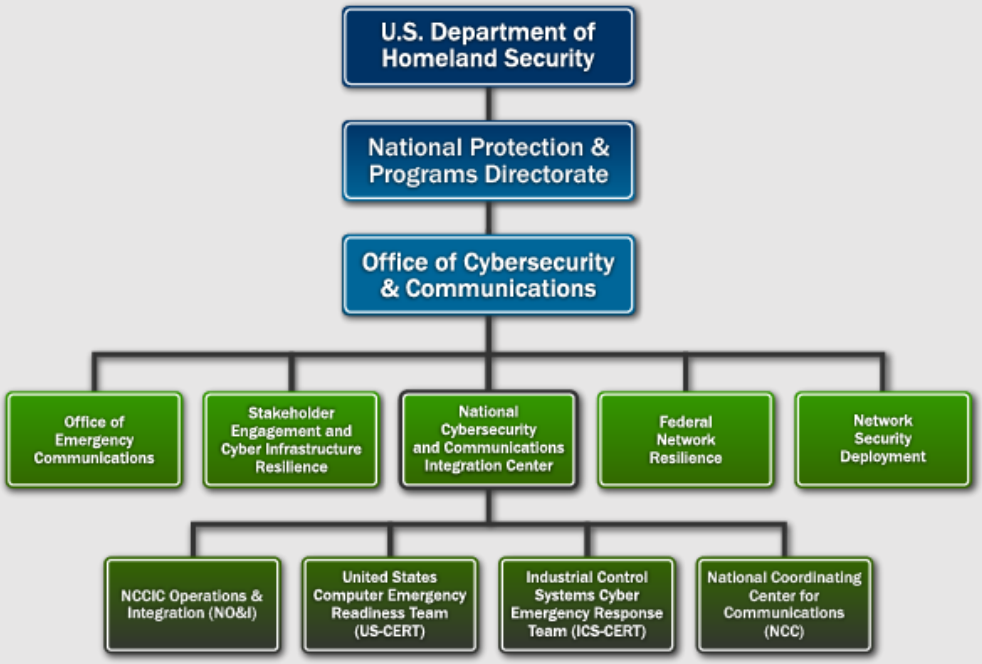
At strategix.xyz we elected to integrate Kaspersky Security Center with IBM Security QRadar as part of our SIEM approach.

IBM Security solutions are built on a framework that spans hardware, software and services. These capabilities comprise a robust set of tools and best practices designed to help address:

1. Intelligence: Through a common and intuitive view that combines deep analytics with security intelligence.

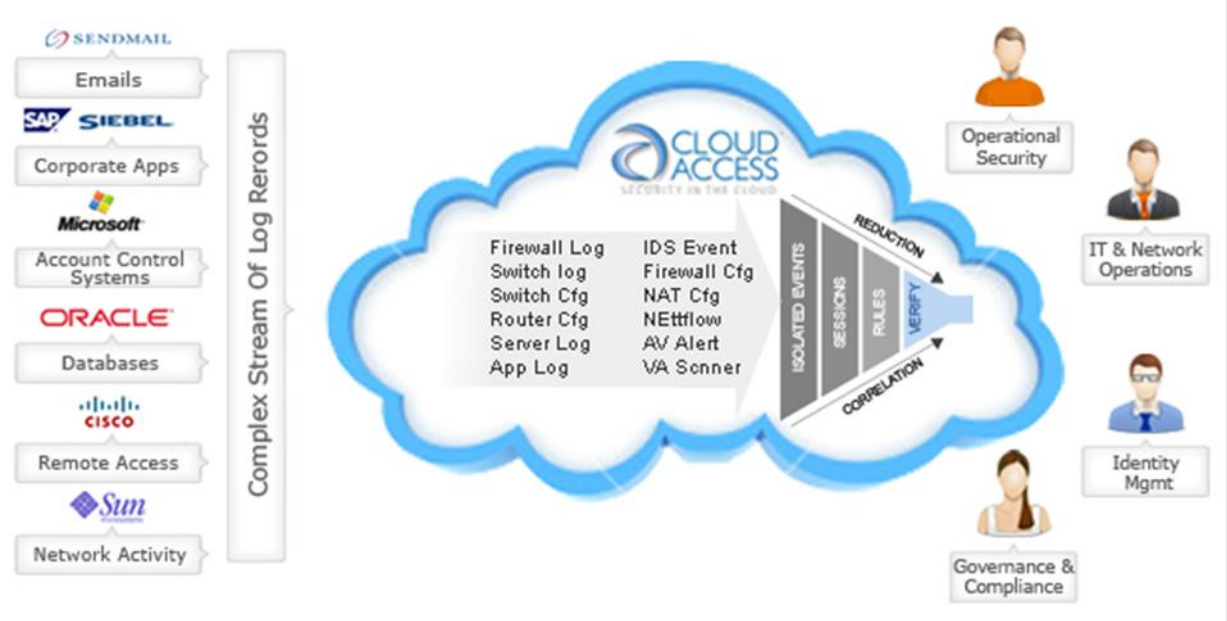
2. Integration: Through unifying existing tools and infrastructures with new forms of defense in order to reduce complexity and lower the cost of maintaining a strong security posture.

3. Expertise: Through a more proactive and trusted source of truth in order to stay ahead of emerging threats and risks.



Organizations that do not collaborate often cite the lack of an information-sharing framework, as well as incompatible data formats and platforms; however, information security managers that do work with others cite clear benefits. Partnerships to enhance security intelligence with collaboration to improve cyber-security and reduce cyber-risks augment information security capability. Most organizations say external collaboration allows them to share and receive more actionable information from industry peers, as well as **Information Sharing and Analysis Centers** (ISACs), government agencies and law enforcement. Many also say information sharing has improved their threat awareness. By sharing, partners get threat information and tools they otherwise might not have access to. They also enhance their network defense by leveraging the cyber experiences and investments of their partners. Sharing can be particularly beneficial in cyber defense because threat groups attack sectors differently, using different tactics and techniques. A number of groups have formed or are forming to share cyber threat information. While some of these groups restrict membership by sector (such as defense industrial base or financial services), others have broad-based memberships.

Additionally, we work closely with the Department of Homeland Security to build a more secure national cyber ecosystem by involving private firms, non-profits, governments, and individuals in countering cyber-attacks. DHS's **National Cyber-security and Communications Integration Center** (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigation best practices. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.



Just as the top cyber-security executive has become more involved in a wider range of activities, so too has the Board of Directors, with an uptick in Board participation in most aspects of information security.

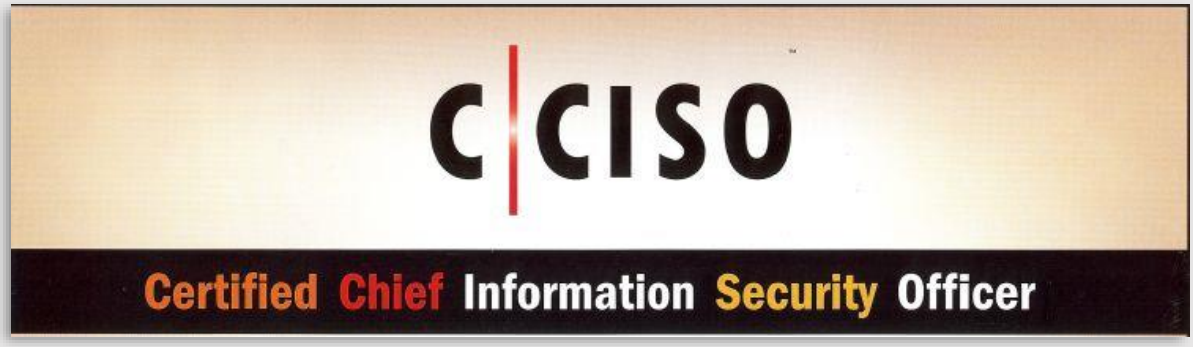
This deepened Board involvement has helped improve cyber-security practices in numerous ways. Perhaps the most striking is Board participation in information security budgets, which may have contributed to this year's significant boost in security spending, authorizing projects with a sound business case.

Other notable outcomes include identification and awareness of key risks, helping foster an organizational culture of security, and better alignment of information security with overall risk management, business process, and business goals.

About 58 percent of cyber security incidents in the public sector were caused by employees, according to this year's annual Verizon Data Breach Investigations Report. Most were caused by employee accidents and incompetence in handling data; however, 1 in 5 internally generated incidents were by unapproved or malicious data use.

The public sector is much more deliberate to report incidents than the private sector; however, industry experts suggest that similar results can be expected in the realm of private data breach. Much of the focus has been to keep external threats at bay; and internal mismanagement or misuse was assumed to require minimal attention.

That too has changed. Managers with sensitive information or data must take precautions to protect that information and keep it from unethical intentions. A culture of security is paramount for an organization to realize an effective enterprise risk management (ERM) policy.



Cyber-security is now on the forefront of strategic issues being addressed at the highest levels of every business meeting. HRM professionals are requesting additional organizational resources be invested in security awareness, policy, and procedures.

Technological advances are very impressive and can distract leaders from continuing to keep the focus on the cyber-security competencies and on-going training of people; therefore, it is encouraging to find that top security executives and Boards of Directors are playing increasingly prominent roles.

Administrative best practices include hiring a Chief Information Security Officer (CISO) to be in charge of the security program and to work as a partner with the HRM function.

The CISO is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected.

The CISO is a separate member of the technology team with a different role from the CIO. Regardless of title, the roles and responsibilities of the top cyber-security executive have expanded in recent years.

Today's CISO is a business manager who should have expertise not only in security but also risk management, corporate governance, business operations and overall business objectives. The CISO responsibilities includes developing, articulating and delivering a business-aligned security and IT risk management strategy.

EC-Council's CCISO Program has certified leading information security professionals around the world. The EC-Council CCISO Body of Knowledge covers all five the CCISO Information Security Management Domains in depth and was written by seasoned CISOs for current and aspiring CISOs.

Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.

Data security is a major issue for businesses and organizations today. Ensuring that your data is secure is becoming more important every day and vital to business operations. A report from CDW showed that data loss has emerged as the top cyber security challenge that medium and large businesses are now facing.

Data Security is the practice of keeping data protected from unauthorized access and corruption. The focus behind data security is to provide privacy while protecting personal or corporate data. Data is the raw form of information stored in databases, network servers and personal computers. This may be a wide range of information from personal files to intellectual property to market analytics and details intended to be private. Data loss damages organizations in a large variety of ways and is expensive, with estimated costs around $200 per record breached; an average of $6.8 million per total breach. A number of high-profile breaches outline this concern.

While data breaches and attacks are of high concern, they aren't the only risk. Many forget the impact that natural disasters have on data security. Fire, flooding, and other natural disasters can destroy valuable data and jeopardize business continuity.

Data Security is critical for most businesses and even home personal computer users. Client information, payment information, personal files, and bank account details are all types of information that can be hard to replace and potentially dangerous if it falls into the wrong hands. Organizations must take a holistic approach to protecting their information across the enterprise in physical, virtual and cloud infrastructures by:

- Understanding where sensitive data exists
- Safeguarding sensitive data in both formats
- Protecting non-production environments
- Securing and continuously monitoring access to the data
- Demonstrating compliance to pass audits

All have varying impacts on an organization’s sustainability, yet management can assess and survive all these risks and more by preparing for adversity or seizing opportunities within an **Enterprise Risk Management** (ERM) framework.

“The mantra of any good security engineer is: 'Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.” — Bruce Schneier

Data Security & Enterprise Risk Management

Key to the availability of information is an organization's backup and recovery strategy and solution. Without the ability to recover data in the event of loss, organizations can be left without the ability to do business, both in the short- and the long-term.

Organizations are currently faced with the task of dealing with an ongoing data explosion. As the need for increased data capacity continues to grow, more and more enterprises are migrating portions of their storage, as well as workloads, into cloud-based data centers. In addition, virtualization is a growing trend, pushing further services, applications and therefore data into the cloud.

The result is that a large number of organizations have now adopted a hybrid model, with data spread between on premises and cloud-based solutions. However, many businesses have not addressed their information management requirements accordingly. The need to ensure that data backup and recovery solutions support a cloud and hybrid environment is becoming increasingly critical to business continuity and sustainability today.

It is, therefore, essential in an increasingly cloud-based environment to ensure the effectiveness of backup and recovery operations that utilize cloud storage services.

Becoming much more mainstream, cloud-based applications offer a great level of data security (data centers with high-level, built-in security and redundancy while addressing the business continuity question at the same time. Work from anywhere, anytime, even after a catastrophic event at the office. There is clear value in cloud.

While many organizations have dealt with the obvious concerns like secure online back-up, secure network communications, servers kept in secured spaces or compliance with certain initiatives, the more subtle, yet potentially more important, data is right there in front of us and we don't usually notice it in our information technology strategies: paper documents.

Appropriate document management cannot be overlooked. There is a growing realization for secure document management and destruction as a preventative measure against information security breaches. While there are no sure-fire methods for preventing security breaches from within, there are ways to reduce the threat – and creating a total security culture is one of the key components of any successful strategy.

"Espionage, for the most part, involves finding a person who knows something or has something that you can induce them secretly to give to you. That almost always involves a betrayal of trust." - Aldrich Ames

Effective information technology and data security strategies should account for all data and seek to bring unstructured data into the structured world for easier inclusion in the overall information technology strategy.

Two types of data; structured and unstructured. Unstructured data is a generic label for describing data that is not contained in a database or some other type of data structure.

Text messages are unstructured data that is generated in media like email messages, PowerPoint presentations, Word documents, collaboration software and instant messages. A comprehensive data security solution will protect both types of data to some degree. Obviously, insider betrayal is very difficult to predict ... and always will be.

Hillary Clinton, as Secretary of State, was sending sensitive diplomatic information to a non-Federal employee's AOL account. Which got hacked. The fact that Sydney Blumenthal's email account got hacked and we know about this stuff is proof in and of itself of why there are security protocols that should have been adhered too.

In addition to being potentially illegal, it was incredibly careless. By using a separate non-government server and set of email addresses, it was easier to duck Freedom of Information Act (FOIA) requests and inquiries by oversight / adversaries / journalists / investigators. However, she is on our team.

FBI Director James Comey stated, “Although we did not find clear evidence that Secretary Clinton or her colleagues intended to violate laws governing the handling of the classified information, there is evidence that they were extremely careless in their handling of very sensitive, highly classified information.”

Once the personal email server was spun-up, no third party was archiving the communication, nor could be fully involved in a check for veracity or completeness without her letting them do so. No political enemy or ally or neutral party could reach into her electronic correspondence, period, to see anything she didn't want them to see. It would be entirely up to her, not a third party, to supply relevant data.

"At a minimum, Secretary Clinton should have surrendered all emails dealing with Department issues before leaving government service," says an audit by the State Department Inspector General, "Because she did not do so, she did not comply with the Department's policies that were implemented in accordance with the Federal Records Act."

To me, by spinning up a separate server, not complying with lawful FOIA requests, lying repeatedly to the American public about it, stonewalling the press, refusing independent review, deleting 30,000+ emails, wiping the server in the face of Congressional subpoenas and having a key IT person who was involved with the server take the 5th about it, she loses the benefit of the doubt from reasonable voters. It is, however, a betrayal of our duties as citizens, to not demand proper conduct from an official merely because they are "on our team." This woman is not fit to be promoted, for this and myriad other clandestine conduct.

Data Security & Enterprise Risk Management

Enterprise risk management helps a company get to where it wants to go and avoid pitfalls and surprises along the way.

The capability inherent in ERM helps management to achieve the performance and profitability targets as well as prevent loss of resources. This helps provide effective reporting, compliance with laws and regulations, and helps to avoid damage to a company's reputation and associated consequences.

Management sometimes assumes that when they have identified and summarized the top risks to their organization through a Strategic Risk Assessment, they have implemented ERM. This is simply not the case; however, a Strategic Risk Assessment is an important component of ERM and usually a starting point, but should not be considered a final destination.

Thorough data security begins with an ongoing program of comprehensive strategy and risk assessment. This will enable an organization to identify the risks being faced with and what could happen if valuable data is lost through theft, malware infection, errors, incident, or a system crash.

While each and every organization has unique security challenges, the top five security concerns among organizations, according to the TELUS and Rotman survey on security breaches, are related to:

- Disclosure or loss of confidential data
- Compliance with regulations and legislation
- Business continuity and disaster recovery
- Loss prevention of strategic corporate information
- Understanding and compliance with security policy

A lack of a strategic security planning, combined with weak or inconsistent implementation of an organization's security policies and procedures, creates an organizational environment that is more susceptible to security breaches.

The culture shift towards total security, therefore, should start at the very top with the adoption of high-security strategic thinking among the senior management team, who can then push it down the organization in the form of effective security policies, processes and values.

Increased connectivity and data access have greatly heightened the risk of a major security breach; therefore, on top of the requisite technological protections, one of the best practice security defenses organizations can have is a "culture of security."

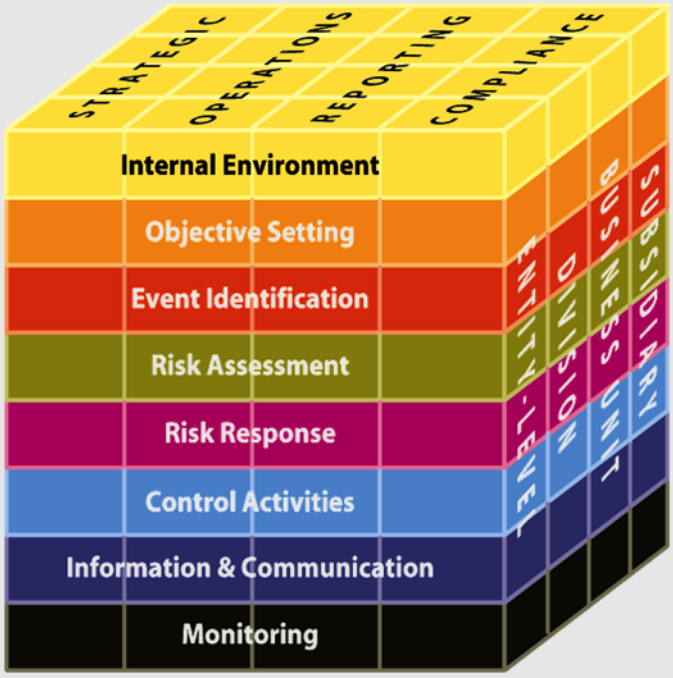
Organizations can turn to the **COSO ERM framework** to identify areas of vulnerability and develop strategies for securing your data and information systems.

ERM includes the methods and processes used by organizations to manage risks and achieve their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.

After the enterprise risk analysis, you can then prioritize specific data along with your more critical systems and determine those that require additional security measures. It is also a good idea to layout a BCP (Business Continuity Plan) so that your staff is still able to work effectively if the systems happen to fail. Company risks and security implementations should be reviewed frequently to support changes such as the growth of your business and other circumstances.

By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

In response to a need for principles-based guidance to help entities design and implement effective enterprise-wide approaches to risk management, COSO issued the Enterprise Risk Management – Integrated Framework in 2004.



This framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.

Additionally, the 2013 Internal Control - Integrated Framework is expected to help organizations design and implement internal control and management oversight in light of myriad changes in business and operating environments. This extended framework is to realize the application of internal control in addressing operations and reporting objectives, and clarify the requirements for determining what constitutes effective internal control.

> "The essential problem is that our models—both risk models and economic models—as complex as they have become, are still too simple to capture the full array of critical variables that govern global economic reality." - Alan Greenspan

Control Objectives for Information and Related Technology (COBIT) is a framework developed in the mid-90s by ISACA, an independent organization of IT governance professionals. ISACA currently offers the well-known Certified Information System Auditor (CISA) and Certified Information Security Manager (CISM) certifications. This framework started out primarily focused on reducing technical risks in organizations, but has evolved recently with COBIT 5 to also include alignment of IT with business-strategic goals. It is the most commonly used framework to achieve compliance with Sarbanes-Oxley rules.

COBIT is used globally by all managers who are responsible for the IT business processes. It is a thoroughly recognized guideline that can be applied to any organization across industries. Overall, COBIT ensures quality, control and reliability of information systems in organization, which is also the most important aspect of every modern business.

Ingraining COBIT 5-based auditing into the organizational DNA is critical to building a secure IT environment that is closely aligned to changing business realities. Organizations that establish a COBIT-oriented auditing approach are better positioned to comply with IT regulatory requirements in a sustainable manner, and drive better value for their enterprise.

Every company with trade secrets and competitive advantage is being targeted, secretly and deliberately, by both insider and external spies. Protecting trade secrets and competitive advantage must be an immediate top priority in all organizations with the highest level of aggressiveness.

BlackOps Partners Corporation, which performs counterintelligence and protection of trade secrets and competitive advantage for Fortune 500 companies, estimates that $500 billion in raw innovation is stolen from U.S. companies each year. Raw innovation includes trade secrets, research and development, and products that give companies a competitive advantage.

Industrial espionage is the theft of trade secrets by the removal, copying or recording of confidential or valuable information in a company for use by a competitor. Economic espionage is conducted for commercial purposes rather than national security purposes, and should be differentiated from competitive intelligence, which is the legal gathering of information by examining corporate publications, market environment, patent filings and the like, to determine a corporation's activities.

Obviously unethical, espionage includes covert activities, such as the theft of trade secrets, bribery, blackmail and technological surveillance. Industrial espionage is most commonly associated with technology-heavy industries, particularly the computer and auto sectors; however, food and pharmaceutical industries are included, all of which a significant amount of money is spent on research and development (R&D).

A Washington think tank has estimated the likely annual cost of cybercrime and economic espionage to the world economy at more than $445 billion — or almost 1 percent of global income.

The estimate by the Center for Strategic and International Studies is lower than the eye-popping $1 trillion figure cited by President Obama, but it nonetheless puts cybercrime in the ranks of drug trafficking and human trafficking in terms of worldwide economic harm.

The U.S. government intends to increase its law enforcement efforts to fight what officials call a surge in corporate economic-espionage cases. The FBI’s counterintelligence division suspects that much of the suspicious activity is performed by Chinese companies against U.S. firms and that the Chinese government plays a significant role in the attempted theft of trade secrets.

Due to the nature of the business, transparency equates to negative publicity, so management is not pursuing litigation; therefore, it is often difficult to place solid numbers on the cost of economic espionage. To protect their investors, companies rarely want to announce breaches by spies or hackers to the public, and government agents often find gathering enough evidence to charge an insider with espionage difficult.

> Chinese proverb: It is only the enlightened ruler and the wise general who will use the highest intelligence of the army for the purposes of spying, and thereby they achieve great results. - Sun Tzu

While copyright and patent law are enforced within our boarders, other countries do not see infringement or duplication as a violation; but rather, as a means to increase their domestic product and quality of life. The Chinese conduct industrial espionage as part of normal business; however, typically engage in spying with low-key or even clandestine tactics.

Really, almost every country is hoping to duplicate the successful economic model of the USA / Canada and sees industrial espionage as a means to an end. Therefore, every successful business in North America is a target, and their source of competitive advantage is the treasure.

The goal of competitive intelligence, ultimately, is to reduce anxiety about making decisions under uncertainty and with limited information. Domestic competition will employ research analysts to compile an intelligence report on factors that influence market performance. For example, while one men’s clothing retail operation is thriving, another is sinking, and the executives in peril want to know what they’re doing wrong (what the competition is doing right).

Gartner estimates the business-intelligence market at about $30 billion, of which Competitive Intelligence (CI) might arguably be considered a small slice. CI is usually within the purview of marketing departments. The largest companies with aggressive CI practices in highly competitive industries--Oracle, IBM, Microsoft, and Procter & Gamble come to mind--have entire departments devoted to the mission.

There has to be a focus on actionable intelligence, the kind of information that lets you make decisions. Clients reach out for help with a competitive-intelligence problem because they're confused and, perhaps, afraid of making the wrong strategic decision.

Overall, near-term prospects favor greater information security. True, closed systems are continuing to open up and the number of opportunities for waging computer warfare continues to rise. Yet, protection tools are becoming better, the Internet is likely to become more secure, the costs of backup and redundancy are likely to fall sharply, and cryptographic methods are likely to spread.

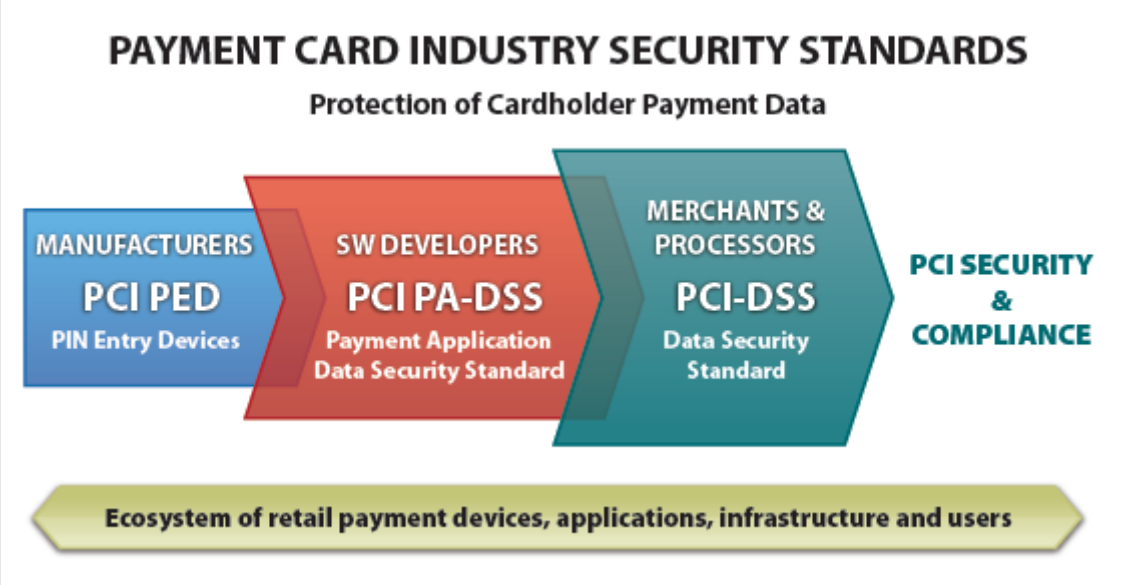
Cyber threats come from criminals that use highly sophisticated methods to breach corporate systems and steal valuable Data. Meaning Internet Data Security is more important than ever. Actually 510 million corporate records were reported breached in 2014. A cyber-attack can steal Data from your Data network over a long period of time.

So much has been spoken, written and frankly overhyped about Big Data in recent years that the most important considerations with regard to Big Data might seem to be: what to believe, and where to start. Actually, IT and Data science teams deploying Data management solutions are expressing great confidence in security assurance with regard to Big Data in the cloud.

Data is the lifeblood of today's digital businesses. Protecting it from theft, misuse, and abuse is the top responsibility of every security and risk management leader. Hacked customer data can erase millions in profits, stolen intellectual property can erase competitive advantage, and unnecessary privacy abuses can bring unwanted scrutiny and fines from regulators while inflicting reputational damage.

Almost every firm, from an online retailer to a hospital to a government agency, rarely works in isolation and can rarely confine data to within their four walls. The walls don't exist. They must work in a complex ecosystem of customers increasingly concerned about their privacy, digitally native employees, and demanding partners and suppliers — all perpetually connected by new systems of engagement and cloud services.

In this new reality, traditional perimeter-based approaches to security are outdated. Security and risk management pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model. Security and risk management pros who take this approach will help their firm position data security and privacy capabilities as a competitive differentiator and build a new kind of customer relationship.



Industry experts recognize there's no single solution that addresses all security challenges. The fact is, security requires a daily coordinated focus on people, process and technology.

The **PCI Data Security Standards**, which encourage a multi-layered approach to data security, along with technology innovations and greater law enforcement efforts represent the future in this ongoing battle to protect consumers' confidential information from the bad guys.

The Payment Card Industry Security Standards Council (PCI SSC) develops and manages the PCI standards and associated education and awareness efforts. The PCI SSC is an open global forum, with the five founding credit card companies -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. -- responsible for carrying out the organization's work.

The breach or theft of cardholder data affects the entire payment card ecosystem. Customers suddenly lose trust in merchants or financial institutions, their credit can be negatively affected -- there is enormous personal fallout. Merchants and financial institutions lose credibility (and in turn, business), they are also subject to numerous financial liabilities.

Following PCI security standards is just good business. Such standards help ensure healthy and trustworthy payment card transactions for the hundreds of millions of people worldwide that use their cards every day.

Organizational Strategy: ***Data Driven Decision Making***

Big data is a collection of data from traditional and digital sources inside and outside your company that represents a source for ongoing discovery and analysis.

Unstructured data comes from information that is not organized or easily interpreted by traditional databases or data models, and typically, it's text-heavy. Metadata, Twitter tweets, and other social media posts are good examples of unstructured data.

Multi-structured data refers to a variety of data formats and types and can be derived from interactions between people and machines, such as web applications or social networks. A great example is web log data, which includes a combination of text and visual images along with structured data like form or transactional information.

Every enterprise needs to fully understand big data – what it is to them, what is does for them, what it means to them –and the potential of data-driven marketing.

Once you start tackling big data, you'll learn what you don't know, and you'll be inspired to take steps to resolve any problems. Best of all, you can use the insights you gather at each step along the way to start improving your customer engagement strategies; that way, you'll put big data marketing to work and immediately add more value to both your offline and online interactions.

> "Information is the oil of the 21st century, and analytics is the combustion engine."
> – Peter Sondergaard [Gartner]

Big data is a popular term used to describe the exponential growth of data collection and analysis that is as important to business as the creative talents because more data may lead to more accurate analyses. More accurate analyses may lead to more confident decision making. And better decisions can mean greater operational efficiencies, cost reductions and reduced risk.

The emerging phenomenon called big data is forcing numerous changes in businesses and other organizations. Many struggle just to manage the massive data sets and non-traditional data structures that are typical of big data.

Others are managing big data by extending their data management skills and their portfolios of data management software. This empowers them to automate more business processes, operate closer to real time, and through analytics, learn valuable new facts about business operations, customers, partners, and so on.

The result is **Big Data Management** (BDM), an amalgam of old and new best practices, skills, teams, data types, and home-grown or vendor-built functionality. All of these are expanding and realigning so that businesses can fully leverage big data, not merely manage it. At the same time, big data must eventually find a permanent place in enterprise data management.

> "Big data is not about the data" – Gary King, Harvard University, making the point that while data is plentiful and easy to collect, the real value is in the analytics.

Big data technologies are maturing to a point in which more organizations are prepared to pilot and adopt big data as a core component of the information management and analytics infrastructure.

Big data, as a compendium of emerging disruptive tools and technologies, is positioned as the next great step in enabling integrated analytics in many common business scenarios. As big data wends its inextricable way into the enterprise, information technology (IT) practitioners and business sponsors alike will bump up against a number of challenges that must be addressed before any big data program can be successful.

Five of those challenges are:

1. Uncertainty of the Data Management Landscape – There are many competing technologies, and within each technical area there are numerous rivals. Our first challenge is making the best choices while not introducing additional unknowns and risk to big data adoption.

2. The Big Data Talent Gap – The excitement around big data applications seems to imply that there is a broad community of experts available to help in implementation. However, this is not yet the case, and the talent gap poses our second challenge.

3. Getting Data into the Big Data Platform – The scale and variety of data to be absorbed into a big data environment can overwhelm the unprepared data practitioner, making data accessibility and integration our third challenge.

4. Synchronization Across the Data Sources – As more data sets from diverse sources are incorporated into an analytical platform, the potential for time lags to impact data currency and consistency becomes our fourth challenge.

5. Getting Useful Information out of the Big Data Platform – Lastly, using big data for different purposes ranging from storage augmentation to enabling high-performance analytics is impeded if the information cannot be adequately provisioned back within the other components of the enterprise information architecture, making big data syndication our fifth challenge.

“You can have data without information, but you cannot have information without data.” - Daniel Keys Moran

While there is broad industry consensus on the value of Big Data, there is no standardized approach for how to begin a program and complete a project.

The myriad tools, vendors, and best practices in the marketplace, multiplied by different use cases and potential projects, can lead to decision paralysis. Additionally, some organizations mistakenly focus on technology first instead of business objectives and requirements discovery.

All of these factors put every Big Data project at risk. In a recent survey of IT professionals, it was found that nearly 55% of Big Data projects don't get completed. Furthermore, only 25% of those projects realize the intended value, such as developing actionable information.

While how you manage your Big Data project will vary depending on your specific use case and company profile, there are 4 key steps to successfully implement a Big Data project:

1. Defining your business use case with clearly defined objectives driving business value and aligned with organizational strategy.

2. Planning your project with a comprehensive plan and scope will lead to success; as well as executing the project with effective leadership and competent management.

3. Defining your technical requirements as detailed requirements will ensure you build what you need to reach your objectives.

4. Creating a "Total Business Value Assessment" as a holistic solution comparison will take the politics (and emotion) out of the choices and exploit objective decisions.

Big Data and the Human Element

Organizations, by and large, still struggle to derive value from data and analytic initiatives, according to Forbes Insights research, Analytics: Don't Forget the Human Element — Data and Analytics Impact Index.

Companies "must contend with organizational resistance, processes, incentive systems, skills mismatches and other factors that are essential to achieving greater buy-in for analytics-driven approaches," according to the report. "Enterprises are beginning to address these challenges by recognizing the importance of change management and forming teams or centers of excellence to elevate these initiatives across the entire organization."

HR is in the perfect position to be big data's center for excellence. Thanks to technological advancements, HR can now expand from traditional roles emphasizing compliance and internal people enablement to taking on more transactional enablement challenges that impact customers and other external stakeholders.

Technology is changing HR. But HR can also help change how people in organizations gather and use data produced by new technological innovations. Without a doubt, analytics and big data can mean sounder decision-making, impactful leadership and increased business value.

Technology is part of the solution. But we cannot forget the human element. And that's where HR can excel the most.

The term 'Big Data as a Service' may be rather unwieldy and inelegant but the concept is rock solid. As more and more companies realize the worth of implementing Big Data strategies, more services will emerge to support them. Data analysis can and generally does bring positive change to any organization that takes it seriously, and this includes smaller scale operations which won't have the expertise (or budget to develop that expertise) to do it themselves.

With the growth in popularity of BDaaS, we are increasingly used to working in a virtualized environment via a web interface, and integrating analytics into this process is a natural next step. We can already see that it is making Big Data projects viable for many businesses that previously would have considered them out of reach – and I think it is something we will see and hear a lot more about in the near future.