tracesecurity
Compliance, simplified.

White Paper

Five Critical Components for a Risk-Based Information Security Program

An integrated, cloud-based approach to data security and compliance.

Executive Overview

As technology and the information age continues to propel organizations forward at a faster and faster pace, risk-based information security concerns must be top-of-mind for not only IT staff but also executive management. The high speed at which information is shared increases the possibility of a data breach. To keep up, state and federal laws are ever-changing and continue to impose stricter obligations to protect the data that an organization collects, stores, processes, uses and discloses.

A significant percentage of large businesses have taken heed, as the decades-long mantra from information security experts recommended, and invested enough in security to make it difficult, risky and expensive for cyber criminals to attack. In search for an easier target, small- and medium-sized organizations have now become the target of choice.

According to CSO Online's May 2012 article, Thwarted by security at enterprise, cyber criminals target SMBs, "Verizon's security research director, Wade Baker, said SMBs are 'easy targets' for organized cybercrime compared with larger enterprises. 'Cyber criminals have figured out that if their goal is to make money, attacking a large organization, that's well-defended and probably has ties to law enforcement, is a high-risk solution,' he said. On the other hand, a mass-produced commoditized attack against small organizations with fewer defenses is 'very low risk'."

In addition to the rising rate of threats on smaller organizations, regulatory requirements continue to add pressure. It is obvious that they don't have the same level of resource, but they can no longer simply afford to ignore the risk or compliance regulations of their industry. Organizations that face growing legal obligations must learn how to comply with and manage the many laws and regulations on an on-going basis.

So, what choice do organizations have? All of the current market solutions have been built to protect the largest enterprises and are too complex and costly for smaller organizations to manage. According to Mark Baldwin, principal researcher and consultant for InfosecStuff, smaller organizations can afford significant protection with a "risk-based approach to threat management." In addition, when organizations approach compliance in an integrated fashion, it becomes manageable. Today, most organizations do not have the knowledge or tools to manage their compliance and often results in efforts that are incomplete, redundant, inadequate and expensive.

In a recent study conducted by SC Magazine with 527 SMBs across various industries, only half of the organizations who placed importance on protecting their Confidential Data and Complying with Standards and Regulations felt that they were capable to do so. This does not have to be the case for the future. It is inevitable the all organizations will demand a solution that meets their needs and enables them to implement a comprehensive risk-based information security program. As products begin to enter the market, organizations must require that their key needs are being met and truly allow them to easily manage an on-going risk-based information security program.

This paper will discuss five key components any risk-based information security software solution must include to best help organizations position themselves to protect confidential information and to meet the regulatory requirements of their industry.

1. A single, comprehensive and integrated solution
2. Database engine of regulations and citations
3. Built-in security expertise and permission-based access
4. Risk scoring
5. Compliance by default

1. A Single, Unified and Comprehensive Solution will Deliver a Manageable and Ongoing Information Security Program.

Solutions in the market today typically provide a piecemeal approach to security and compliance. Not only is it incredibly expensive to implement all of the necessary components for a complete information security program, it also requires security expertise to manage the disparate systems because they were not built to seamlessly communicate.

For example, when data is placed into a risk assessment point solution, it will have to be re-entered numerous times, within the individual audit and policy management systems (just to name a few). Only the largest organizations with the largest IT resources and security expertise have the time and ability to manage such an undertaking. If all of the necessary functional areas were integrated into a single, comprehensive solution it would eliminate those redundancies and significantly reduce the total cost of ownership.

Efficiency would increase dramatically if once an organization completed its risk assessment the data was intelligently pre-populated and filtered into the rest of the functional areas of the software, resulting in streamlined audit, policy, process, vendor, vulnerability, compliance, BIA/BCP, incident response and training management.

Once a unified approach to risk-based information security is adopted, SMBs will be able to easily and effectively manage the growing number of information security compliance requirements. A truly comprehensive solution will:

- Identify your organization's risk
- Identify the controls to mitigate that risk
- Map regulatory requirements to controls to facilitate compliance by default
- Tell your organization which controls are already in place
- Develop a plan to implement missing controls based on their cost effectiveness
- Report on governance functions and compliance

In order for a solution to be comprehensive, it must offer end-to-end functionality that includes risk, process, policy, vulnerability, training, vendor, audit and compliance management.

Risk Assessment Score Card	
Action	**Result**
Has not performed a risk assessment and does not have a plan to address risk.	Uses its security budget to implement the latest and greatest security tool with little regard to whether it addresses a security risk for the company and does not consider the risk's criticality.
Has performed a risk assessment and may have plans to implement tools, policies and/or processes to address the risk.	The organization does not have the time, resources or security expertise to implement the required controls.
Has performed a risk assessment and believes it has implemented the appropriate controls.	The organization has never audited the controls to confirm that they are truly implemented. For example, they have never tested the policy controls to ensure employees follow them.
Has performed a risk assessment, implemented controls and audited the controls – two years ago.	In the meantime, the organization has reorganized, implemented mission-critical software and opened two new locations. The organization does not have an on-going plan and continues to allocate its security budget to controls identified years ago.

"SMBs face a heightened risk, because many lack the wherewithal to recover from the long-run consequences of a serious breach."

Lawrence Pingree, Research Director – Gartner

2. Database of Industry Regulations and Citations that Drives Automation and Streamlines Compliance

Any comprehensive solution should be built around, integrated with and updated regularly to not only your industry-specific regulations but regulations of all industries.

Many industry regulations overlap and an organization may have to comply with multiple information security laws, regulations and guidelines. Because various industry regulations specify or suggest many of the same security risk analyses and management practices, a unified approach streamlines your program and allows your organization to comply with all of them at one time. This ability dramatically eliminates the redundancy of answering the same questions for each regulation.

The database must provide access to not just the regulations, but also the authority documents and citations within. As regulations are chosen and controls are applied, all of the associations for every regulation become accessible with accompanying documentation.

Most often, business owners aren't experts in regulations. If the business owner can see each of its controls and easily drill down into the guidance that it addresses, they don't have to be experts to determine what needs to be done next.

3. Built-In Expertise that Enables Permission-Based Access, Management and Reporting

Solutions currently in the market are built by security experts for security experts and do not address the needs of most organizations that do not have security expertise on staff or the resources to manage complex information security programs.

Organizations that have performed a risk assessment know their risk. They may even have a plan to implement the tools, policies and/or processes that address that risk. But, that organization may also find it does not have the time, resources or the security expertise to dedicate to the implementation of the required controls.

The answer is a solution that automates and guides control implementation, thereby, reducing the resource or expertise required to implement and manage the risk. A solution with inherent security knowledge allows staff, who are not security or technology experts, to access and contribute to areas of the system for which they do have functional knowledge, such as HR and legal – spreading tasks among divisions and other areas of the organization and taking the burden off of a single individual.

With a permission-based solution, an organization's individual employees, an entire department or even a third-party vendor can be assigned and become responsible for assignments that directly relate to their role and functional expertise. For example, an organization can associate and assign controls to a specific vendor. This allows the organization to best understand its risks, as they relate to that vendor relationship, report on and provide the vendor oversight that is necessary to confirm they have properly managed and completed their assigned controls.

If a solution does not provide guidance to the employee on how to perform the necessary tasks, it is not built with the smaller organizations in mind.

4. Risk Scoring that Optimizes Your Information Security Budget

Today, it is common place that organizations do not perform risk assessments and therefore do not have a plan in place to address risk. The organization likely lacks the knowledge or framework to perform an assessment or doesn't have a solution that helps them manage risk on an on-going basis. This typically leads the organization to be reactive versus proactive, and use its security budget to implement the latest and greatest security tool with little regard to whether it actually addresses a valid security risk for the company.

Once an organization has completed the risk assessment, a comprehensive solution should provide a remediation action plan that is based on a Risk Score. The Risk Score approach to risk assessment allows the organization to measure and report its mitigation effectiveness over time, set benchmarks and analyze trends. Ultimately, this score leads the organization to make better risk-based decisions and optimize its security budget – providing justification for the controls the organization has in place.

For example, Risk Scores change based on controls in place. Organizations can use their Risk Score to make hypothetical changes to their current controls, measuring how the change would affect their score and ultimately drive strategic decisions regarding which controls are most effective for their associated cost.

Helping to streamline the ongoing maintenance of an organization's risk-based information security program, any control changes should automatically update the Risk Score as well as be reflected in the compliance review.

5. Compliance by Default Delivers the Bottom Line

When a comprehensive solution is built around a database of regulations and citations and has the proper risk assessment and audit procedures in place, it streamlines the compliance review process. Activities within every functional area of the system, such as vulnerability management, training, process and policy sign-offs, automatically populate its compliance section and leave the organization with only minimal gaps to fill in the compliance review.

Because mandates are typically met by following best practices that are inherent and built into a comprehensive solution's software, a unified risk-based information security program will organically lead the organization to comply by default and allows them to easily implement and continuously monitor its information security and compliance requirements – all while eliminating the inefficiencies, redundancies and costs that are typical to the market today.

Conclusion

It is essential that organizations migrate to a solution that suits their needs and enables them to make better risk-based decisions, reduce costs, improve security, and report at every level. For the future of information security and compliance success, organizations must establish an information security and compliance vision that is shaped by common sense and proven practices – all with the goal of aligning IT departments with strategic business objectives.

Organizations should avoid solutions that offer standalone components that require aggregation. As regulations become stricter, a risk-based approach to information security will require a manageable but disciplined approach that ties directly to business process and streamlines an on-going program. This translates into greater IT efficiency and dramatically improves an organization's agility to comply. In short, it is your foundation for information security and compliance success that will evolve alongside your organization.

About TraceCSO

TraceCSO is a complete information security, risk management and compliance solution that enables organizations of any size, industry or security skill set to quickly deploy, evaluate, create, implement and manage a comprehensive risk-based information security program – all at an affordable price and without any additional third-party software. Simply put, it is the first and only solution designed to meet the needs of the small and mid-sized business, that also scales to support the enterprise. TraceCSO now makes it simple for organizations to protect its confidential information and meet regulatory requirements, placing priority on information security that organically leads to compliance by default.

TraceCSO provides the sophisticated capabilities you need from an information security and compliance solution, but without the complexity of deployment and resource demands of existing solutions. With an unprecedented level of automation, visibility and access, TraceCSO empowers you to continually ensure the integrity and privacy of your critical data.

About TraceSecurity

TraceSecurity is a leading provider of cybersecurity and compliance solutions that helps organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.