

# IT security:

## Is compliance enough?

If we believe the headlines scrolling across our television sets nearly every week, no one is safe and nothing is secure as it pertains to information technology. The names read like a rogue's gallery – TJ Maxx, Health Net, SAIC, TD AMERITRADE, Forever 21 – all organizations responsible for meeting regulatory compliance standards and protecting sensitive data, yet all victims of massive breaches and exposure that resulted in substantial fines and public relations headaches.

While the list of regulatory compliance measures intended to stem these issues grows, so too does the list of organizations that have failed – many of which had achieved “good-standing” in meeting regulatory compliance obligations. Now, executives responsible for protecting their organizations’ IT assets and reputation are asking: “Is compliance enough?” Clearly, the answer is no, but if compliance is not enough, what is?



# A point-in-time approach to information security generally leads to a time-in-print approach to public relations.

In a 2007 survey by U.K.-based *CIO* magazine, IT chief executives were asked about their concerns. Security and compliance ranked fifth and sixth respectively after people leadership, managing budgets, business alignment, and infrastructure refresh. These results are not surprising, as executives have significant problems to solve in leadership, budget management, and business alignment, and may be influenced by the changing landscape of regulatory compliance and IT security.

Over the last half-decade, a number of new changes regarding security and compliance have transpired, influencing the priority executives assign to information security. Chief among their concerns are:

- The proliferation of threats
- The explosion of technologies to mitigate those threats
- Lack of skilled resources
- Increases in regulatory pressure
- The complexity of leveraging disparate information security systems

In information security and regulatory compliance, the bad guys have all the advantages. Defenders must protect against every possible attack, while attackers need only find one weakness. The immense complexity of modern networks makes proper security a challenge, especially on a limited budget. Furthermore, extranets, virtual private networks, mobile devices, portable media, and more only add to the intricacy.

Skilled attackers can encapsulate their assaults in software, allowing unsuspecting people to use them. Ultimately, these types of attacks prove to be the underlying problem for many organizations tasked with information security and regulatory compliance. Regardless of the volume or stringency of the technology controls put in place, the element of human interaction always challenges security.

# Executives face significant challenges in effectively securing data and meeting regulatory compliance.

Often, executives look to trusted internal resources or third-party consultants to validate that they are in “good standing.” These assessments are an excellent means for ensuring compliance, providing insight into current security posture, and supplying technical direction for building remediation plans and goals.

However, these assessments usually do not include business goals or metrics, the organization’s overall aversion to risk, or integration of technology tools into the business process. The focus is instead on the implementation of the tools, and not the tools’ ability to support business need. This myopic approach significantly diminishes the value the assessment provides to the organization – with the passing of the assessment having far more importance than the information it delivers. This idea of merely checking off the boxes on an assessment, instead of adopting a business culture that prioritizes security and compliance, increases susceptibility to costly security breaches and compliance failures.

When assessments are not performed on a constant and consistent basis, a false depiction of an organization’s risk and liability can develop. This point-in-time approach to ensuring controls for mitigating risk often leads to scandals, loss of confidence and trust by the client base, and in some cases, expensive losses of capital from fines, fees, and services that must be provided to individuals whose data was compromised.

# Information security practice

For businesses competing in today's global market, IT has become the key to unlocking new markets and gaining a competitive advantage. The only thing changing faster than the pace of business in the modern economy is the means by which it is transacted. These advances have powered entire corporations to the forefront of their respective markets; however, they are not without risk or liability. Being first or even the fastest is no longer enough to achieve success. Now, to be market leaders, companies must first ensure the confidentiality, integrity, and availability of the systems they employ. Sarbanes-Oxley, Gramm-Leach-Bliley, and Health Information Portability and Accountability (HIPPA) Acts are but a few of the recent government-enacted programs intended to ensure companies and institutions comply with information security and compliance governance standards.

## Introducing Incentra Information Security Practice and Managed Security Services.

Incentra offers a wide portfolio of services to assist clients in maintaining constant and consistent oversight in their challenge to meet information security and compliance goals. Through a diverse team of information security professionals equipped with managed information security services, Incentra assists clients with overcoming the point-in-time approach to information security and compliance.

The problem is daunting. Companies must maintain the ever-increasing speed of business transactions, while complying with increasingly stringent government and private industry compliance standards – all with a limited budget and resources. Incentra security consultants understand this problem and are uniquely qualified to assist clients with a solution.

Incentra partners with its clients to design, build, and deploy secure, reliable architectures that ensure mission-critical system availability, and improve efficiencies through information technology. Embraced are the ideals defined by the Certified Information Systems Security Professional (CISSP) certification to ensure predictable, high-impact, and cost-effective results:

- **Confidentiality** – The prevention of intentional or unintentional unauthorized disclosure of private information or data.
- **Integrity** – The assurance that modifications to data or information have not been made by unauthorized sources or that unauthorized modifications have been made by authorized sources.
- **Availability** – The assurance that data or computer resources are available in a reliable and timely manner. Availability guarantees systems are up and running when they are needed.

## Information security practice (cont.)

Incentra helps organizations look at the big picture first, to understand how tactical requirements work within strategic business needs, and then ultimately provide enterprise security programs that exceed those expectations.

Incentra consultants' skills range from strategic planning, deployment, and management of advanced systems security architecture, to in-depth review and analysis for the following areas:

- Risk assessments
- Vulnerability assessments and penetration testing
- Social engineering vulnerability assessments
- Enterprise security and privacy program review
- Privacy impact assessments
- Enterprise security assessments
- Regulatory assessments
- Security and privacy program development
- Security and privacy policy creation / revision
- Security / privacy training and awareness
- Security architecture
- Incident response and CERT Program

# Stop throwing technology at a business problem.

Traditional security approaches that required IT executives and managers to research, justify, acquire, install, and maintain multiple security technologies are quickly becoming antiquated, and in many cases, cost prohibitive for their organizations to maintain.

As security threats continue to grow at an exponential rate, and correlatively increasing the remedies designed to address these new threats, executives are realizing this is not a problem that can be solved through technology. Enterprise executives will need partnerships they can trust to meet their information security goals and compliances objectives. In the future, organizations will look to partner with third-party managed services and resources as information security and compliance are migrated to the "cloud."

Incentra is uniquely poised to deliver on the promise of "cloud" security today. Our unique combination of information security and compliance consulting and the GridManage Security platform provides the highest level of protection and flexibility available today. With its subscription-based, pre-integrated security utility offering, Incentra has significantly reduced the time and effort required for addressing pressing security and compliance issues without integration risk or headaches. In leveraging GridManage Security and security consulting expertise, Incentra's clients gain peace of mind in knowing that their information security assets and compliance needs are constantly and consistently managed and vigilantly monitored so that point-in-time does not become time-in-print.

# Contact our sales team

To learn more about Incentra Information Security Practice and Managed Security Services, please contact our sales team at 800.397.1719 or visit [www.incentra.com](http://www.incentra.com).

## Make IT work for you. Choose Incentra.

Whether we're performing selective projects or supplying comprehensive services, we ensure a full array of operational and technical excellence that spans consulting, technology, and outsourcing. We offer a complete menu of infrastructure options, from one-off projects to comprehensive implementations. Learn more about the impact of Incentra. Contact us today to set up an informative meeting.

Sales: 800.397.1719, Technical Support: 877.667.8720, Partner Support: 800.397.1719, email: [info@incentra.com](mailto:info@incentra.com)

---

<b>Corporate</b> 1140 Pearl Street Boulder, CO 80302	<b>Operations</b> 12303 Airport Way, Suite 250 Broomfield, CO 80021	<b>Northwest</b> Portland, OR Kirkland, WA	<b>West</b> San Jose, CA San Diego, CA Santa Clara, CA	<b>Midwest</b> Lombard, IL	<b>South</b> Richardson, TX Houston, TX	<b>Northeast</b> Metuchen, NJ Conshohocken, PA New York, NY	<b>International</b> London
---	---	--	---	-------------------------------	---	--	--------------------------------

[www.incentra.com](http://www.incentra.com)