AT Kearney

The Golden Rules of Operational Excellence in Information Security Management

Efficiency is the next step in the evolution of information security management.

For the evolving field of information security, the adage "knowledge is power" is more apt today than ever before. Information is the currency of today's corporations, and protecting that information is of paramount importance—a company's reputation, strategic relationships, and competitive advantage all depend on it. Digital business models rely on quality and integrity of information as well as the trust of their customers. Therefore, information security is a key success factor of strategic importance for digital business models and, as a result, needs to be analyzed and managed more comprehensively from a corporate leadership perspective.

Better efficiency ensures that information and **intellectual capital is protected—and valuable resources are not wasted.**

What are organizations doing to ensure that they are efficiently, yet effectively, securing their data? To answer this question, A.T. Kearney and the Mannheim Business School surveyed chief information security officers (CISOs).[1] The results of the global study highlight the amount of work to be done in improving the efficiency of information security management—particularly when comparing information security costs with the financial and reputational impact of data breaches. A lack of clarity about how to operate efficiently means that many companies are wasting critical resources in lower-priority areas, resulting in insufficient resources to do the critical work of protecting the crown jewels of the company—their information and intellectual capital.

Striving for Operational Excellence in Information Security Management

The leaders in information security understand what their most valuable information assets are; the potential value that is at risk; the nature and source of threats; the cost of introducing measures to monitor, detect, prevent, and react to information security threats; and how to use their resources—people, technology, time, money—most efficiently to achieve their information security objectives.

Our study indicates that companies are emphasizing the effectiveness of their systems and processes—that is, they're making sure they're doing the job well—yet few use consistent metrics to determine whether they are doing the job efficiently. Seventy-nine percent of respondents say their companies do not have a clear idea about how to define and, therefore, measure the efficiency of their information security processes.

While information security practices are improving across the corporate world, few companies have implemented a model that successfully protects while doing so in an efficient manner. Existing international technical standards and frameworks are available as guidelines for managing information security, yet most fail to address how to do so efficiently.

Ultimately, the business is accountable for protecting its critical information—after all, an information breach can have massive implications across the entire organization and impact their external stakeholders. Wasted resources have a major impact on doing that job well.

[1] In this paper we use the term CISO to refer to the highest-ranking information security person within an organization.

The Golden Rules of Efficient Information Security Management

Efficient information security requires broad, cross-business collaboration that engages the whole company. It requires teamwork, decisive leadership, effective communication, and a culture of continuous improvement. Only then can a company mitigate the information security risks it faces as part of its daily business operations.

In our work helping clients manage their response to information security threats, we recommend the following "golden rules" for achieving successful information security management that is also efficient (see figure 1).

Figure 1

The eight golden rules of efficient information security management

Source: A.T. Kearney analysis

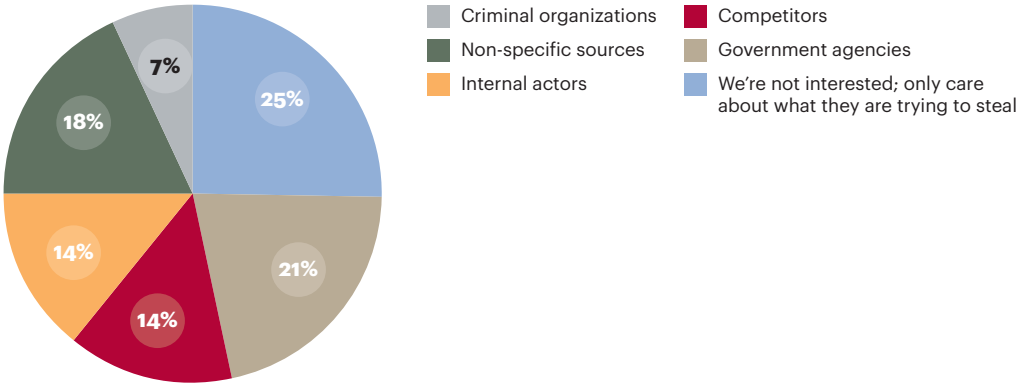
1. Protect your assets according to the value at risk

Information security management "is like a cat and mouse game where you need to be constantly aware of what you are protecting," says Anand Patil, the CIO of education services provider Géant. That means understanding what information assets comprise the "crown jewels" of your organization. Protecting every piece of data is cumbersome and inherently inefficient. Rather, companies need to classify their data based on level of importance, create a security architecture, and set security policies and protection measures for each of these levels. This involves not just assessing the data type and content, but also who has access to the data and the type of authentication needed to view the data. Leading organizations classify their data by engaging a broad group of business stakeholders because, as Dr. Werner Gutau, the head of information security at a leading semiconductor company, puts it, "It is difficult to separate and identify the crown jewels within the company's departments, as it depends on whom you ask."

Classifying and protecting data also requires an understanding of the type and source of threats faced by organizations (see figure 2). Generic attacks target almost all company data and are commonplace, and security measures are usually readily available for most of these attacks. Targeted attacks, on the other hand, are geared toward a particular organization and often a particular data type. Attackers in these types of events tend to put a lot of effort into them; when successful they can have a greater impact on the organization. The leading organizations use psychological analyses to understand the motivations for such attacks so they can prevent and thwart future breaches.

Figure 2

What do you believe are your main information security threat sources?



Source: A.T. Kearney analysis

For organizations dealing with customers' personally identifiable information (PII), preventing breaches is becoming increasingly important, particularly in light of recent and expected changes in legislation and court rulings, and requires a particularly high level of protection. For example, in the Target data breach case, a U.S. federal judge gave preliminary approval to awarding each affected customer up to $10,000. In California, the passage of three separate bills could fine companies that experience a breach a minimum of $2,500 in punitive damages

per customer. With PII, understanding the psyche of the attacker will help in narrowing down the actions required to prevent breaches. This is even more important when it comes to handling internal threats, which constitute a significant risk to companies.

2. Turn your information security department into a business-focused service provider

The leading companies see information security departments as internal service providers. Similar to IT service management, the information security department can create a service catalog that addresses the needs of the individual business departments and hence will be easy to understand. The use of those services will mostly be driven by regulations and security policies; some could even be mandatory. A non-exhaustive list of examples includes:

- Providing a secure environment to a business application managing strictly confidential data
- Third-party security audit
- Security consulting and support to business projects
- Executing annual information security management systems (ISMS) cycle: reviewing risk, measures and implementation planning
- Securing access to public cloud-based services
- Penetration testing and business impact analysis
- Awareness campaigns and staff training

> "There is always a lot of emphasis on information technology and IT architecture. It is often a challenge for many CISOs to exert their influence from the very beginning of a project."
>
> **— Dr. Jörg Bröckelmann, CISO, ThyssenKrupp**

At its core, information security is an extension of the business—and the information security department should provide security services relevant to the business. One way it can achieve this is by acting as a service integrator, combining internally provided services with those delivered by various external service providers. Setting up information security as a shared services center means that costs are allocated based on usage, rather than being rolled into corporate overhead, as is common. When these services show up in each business department's budget, the benefit is not only transparency but also a more efficient use of resources. The objective of the shared service center is to recover the cost of providing services through optimum service pricing. This is particularly important when addressing the issue of cost based on the level of risk and limitation of liability clauses—something that is often ignored in traditional service provider agreements with outsource suppliers.

3. Ensure buy-in from top management

Our research shows that more than half of company CISOs report into the IT department (see figure 3). However CISOs who report directly to a board member tend to work for organizations with more successful information security management departments. As the CISO of a leading bank put it, "It is a good practice when the highest information security officer reports directly to the executive board director. There should not be a layer in between."

If there are intermediate layers in the reporting structure, they should improve board understanding of information security issues and increase transparency rather than obscure it. As Dr. Jörg Bröckelmann, CISO of ThyssenKrupp, noted, "There is always a lot of emphasis on information technology and IT architecture. It is often a challenge for many CISOs to exert their influence from the very beginning of a project."

Our research shows that many boards are proactive when it comes to information security management, although some demonstrate interest only when there is a high likelihood of punishment from a breach (see figure 4).

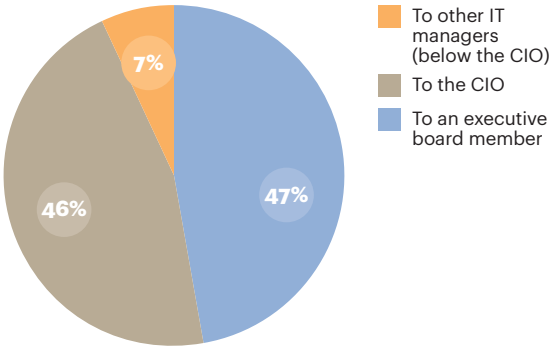
There are several ways senior leadership can underscore the importance of information security management. For example, global software giant SAP has demonstrated its commitment to information security by creating a "human firewall" in which images and promotional materials related to information security, including life-size cutouts, feature board members. Employees are encouraged to take photographs next to the cutouts and post them on the information security blog. This approach signals to employees that leadership is thinking about information security.

4. Establish an information security roadmap with a balanced budget

Every corporation needs to understand its current security posture; align its information security objectives with its business strategy, goals, and value at risk; and then establish a strong and holistic information security strategy with a clear and shared roadmap.

Figure 3

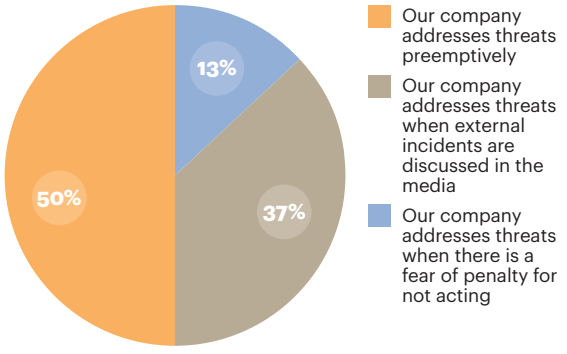
Less than half of CISOs report directly to an executive board member



Source: A.T. Kearney analysis

Figure 4

At what point does your board begin addressing information security threats?



Source: A.T. Kearney analysis

This strategic roadmap and its supporting budget should be regularly updated in response to the threats and changes in the business environment. When security needs can be expressed in financial terms, the board and business lines will be more inclined to pay attention.

Creating a budget to maintain and improve information security capabilities is no easy task. Most information security departments operate under very tight financial constraints. To complicate matters, future needs are uncertain: every year there are new threats and vulnerabilities, new technologies, and often new regulatory requirements. Companies need to walk the line between overspending and underspending, within the context of their risk appetite.

How much should companies be allocating to information security? According to the Gordon-Loeb rule, an organization should never spend more on a security measure than 37 percent of the expected reduction of the risk value through implementation of the measure. Expected loss is based on the value at risk and the probability of the risk materializing. While theoretically sound, this approach assumes a very precise calculation of expected losses, and arriving at such a value is far from straightforward, in particular when evaluating things such as reputation loss.

This is one reason why there is no one-size-fits-all approach to information security budgeting. Companies need to shape their budgets based on business needs. The CISOs we spoke with confirmed this view. Two-thirds say their organizations make allocation decisions based on the requirements for planned projects (bottom-up approach), while one-third said allocations are a percentage of the IT budget (top-down approach). Most CISOs whose organizations used a top-down approach felt a bottom-up approach was preferable.

However, neither of these approaches incorporates all of the costs of information security management. For example, there are additional costs incurred by various departments that are related to information security. Therefore, in order to measure efficiency, information security costs in each of the following budgets need to be taken into account:

a. **Direct.** This budget is usually directly owned by the information security department and covers a variety of areas, from operational activities to risk management, governance, and compliance. For a corporation with a federal information security organizational structure, it includes the group budget as well as the individual budgets for each of the organizational units that have dedicated information security spending.

b. **Indirect.** This budget is usually owned by either the IT department or one of the business departments. It includes the additional costs incurred as a result of information security policies and requirements. Examples could be the cost for IT to develop secure code practices in new applications or the cost of information security controls in business processes.

c. **Emergency.** This is usually handled by senior executives, and funds can be tapped in the event of a breach or incident. The strategies for dealing with emergency funds vary widely across companies; while some CISOs increase the direct budget for worst-case scenarios and shift funds based on the needs of the businesses, others create an entirely separate and dedicated budget for emergencies. Most companies we interviewed had access to additional "as required" contingency funds to limit the damage caused by emergencies or breaches. As Carlos Arglebe, CISO of Siemens Healthcare, put it, "When there are incidents, budgets are not the issue. It's rather having the know-how and being able to figure out and reconstruct the trail and mitigate the damage." This was seconded by a CISO for a leading telecommunications player, who said, "In case of any special event, attack, or breach, we have full backing from the executive committee in terms of financial support. While we don't have a specific contingency provision, we are assured a blank check to fix the issue."

One alternative and innovative approach to funding emergencies is to get the department or the business line that experienced the emergency to pay for it—this improves the accountability of the businesses toward information security, driving both awareness and efficiency. It may also prompt them to consider appropriate cyber insurance options.

It is also important to separate the internal information security budget from those covering product-related information security. In companies with large product divisions these budgets are often handled by a separate team altogether, ensuring a clear demarcation of resources and responsibilities. Also in that case each will have direct and indirect budgets.

Our study clearly indicates a need for delinking the information security budget from the IT budget, and in particular moving away from the widely followed rule of thumb of allocating approximately 5 percent of the IT budget to information security. When budgets are separate there is greater clarity around IT and information security roles, as well as increased accountability for both the CISO and the CIO.

> "It is difficult to arrive at universally reliable KPIs in the security world compared with other domains such as quality."
>
> **— Dr. Werner Gutau, head of information security, leading semiconductor company**

Leading organizations follow a bottom-up approach, developing their strategies and projects first and then allocating budgets based on the planning for the upcoming year. For this to work, there must be a clear prioritization of security measures. For example, "must-have" measures are either required for compliance with laws and regulations, or they are crucial for protecting the company's crown jewels; "almost-must-have" covers the minimal desired protection level—depending on the classification—for all information not covered under "must-have"; "should-have" covers additional protection measures derived from the information security strategy. Everything else becomes "nice-to-have."

A best-practice budget is further divided among preparation, prevention, detection, and reaction measures, with greater emphasis placed on early detection and mitigation versus prevention. The budget should be updated annually—with potential mid-year adjustments driven by unexpected events—rather than simply projected forward, to take into account the financial impact of past incidents and previous security investments, as well as changes in the threat landscape and new protection measures.

5. Use stress and penetration tests periodically

Periodic stress tests, also called war gaming, are designed to assess the potential business impact of attacks. These tests can help companies identify the gaps in their capabilities and can serve as the basis for a remediation plan, including changes to policies, technologies, or even team roles and responsibilities.

A specific way to stress-test a company's security infrastructure is via penetration testing, which uses realistic attack scenarios and vulnerabilities, both technical and non-technical. The results give a clear indication of where investment can create an immediate impact.

When we asked CISOs how many stress tests their organizations carried out annually, responses ranged from once a year—for the purpose of certification—to more than 100 times a year. The optimal number of penetration tests varies according to such factors as company industry, its size and prominence, the geographies in which it operates, and the amount and type of information it handles. Global giants operating in vulnerable industries such as telecommunications, defense, and finance need to carry out penetration tests more often than a regional manufacturing company with limited external exposure. For example, Netflix, as a "high-value target," carries out these kind of tests almost 1,000 times per week. This allows the company to quickly identify loopholes in different functional areas and patch them, clear waste in the system, and assess the health of the overall system.

6. Go beyond benchmarking your peers: Cooperate with them

The respondents in our survey agree that finding universally accepted key performance indicators (KPIs), common in functions such as finance and operations, is nearly impossible in information security. Notes Dr. Gutau: "It is difficult to arrive at universally reliable KPIs in the security world compared with other domains such as quality." In any case, while benchmarking the competition can be helpful for finding new solutions, merely copying other firms' strategies can be ineffective, since good information security management is driven to a large extent by a company's individual business characteristics.

More collaborative efforts can bring greater results for information security teams, in terms of effectiveness and cost reduction. For example, many companies are sharing and comparing information and practices with other organizations, especially industry peers or companies of a similar size (financial or organizational) (see figure 5 on page 9). Sharing best practices can help improve early risk detection and mitigation by reducing the need for experimentation. Our research found that for companies in industries with more experience in information security (such as automotive and finance), as well as those driven by new technology (particularly high-tech firms), there was a greater tendency for competitors to share best practices and collaborate on solutions. The more experienced organizations often collaborate through special—sometimes industry-specific—associations, while technology-driven companies of a similar size often compare tactics and results through neutral collaborative platforms (see figure 6 on page 9).

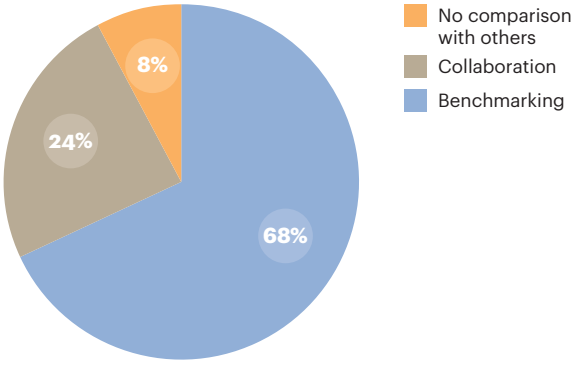
7. Automate processes and functions

Even companies with mature information security practices cannot afford to be complacent. This was echoed by a CISO for a leading global automotive supplier when he said, "Anyone saying he's on top of things in information security should be challenged."

Leading companies stay ahead of the pack by using tools that fully or partially automate security-related functions and processes. Artificial intelligence, machine learning, big data, behavioral analytics, and the like are key trends in the security solutions market. Examples

Figure 5

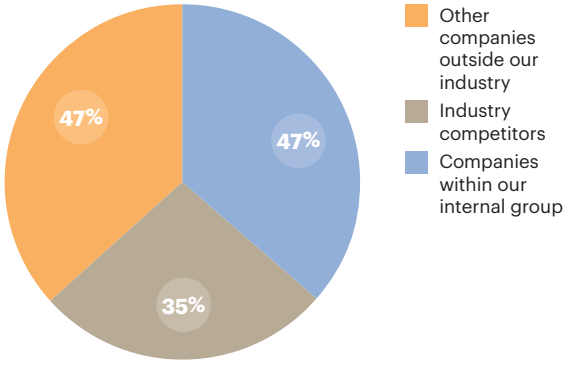
Do you collaborate with or benchmark your information security activities with other companies?



Source: A.T. Kearney analysis

Figure 6

What types of firms do you benchmark against?



Source: A.T. Kearney analysis

can be found in multiple domains, including threat intelligence, vulnerability management, security information and event management (SIEM), information security incident evaluation, and automated penetration testing. These companies improve the effectiveness and efficiency of their security practices by setting up a security operations center (SOC) and integrating these automated solutions. Some have implemented data classification and data leakage prevention (DLP) initiatives that combine manual departmental data classification with automated classification of documents and e-mails based on identification of keywords and pattern recognition. Automated solutions streamline IT security operations by defining the right thresholds, allowing staff to focus on more valuable tasks.

8. Enlist your employees in the fight against breaches

When asked about the most vulnerable aspect of information security management in an organization, one banking CISO said, "The weakest part is always human." Human attitudes and behaviors, which are a reflection of the organizational culture, are a critical element of corporate information security.

In order to increase information security effectiveness, mandatory training and awareness campaigns are imperative. Vanessa Hanke, director of global security policy and standards at SAP, said, "You can have as many standards as you want, you can have as many technological checks, but awareness among the workforce remains critical."

How the average worker views information security drives its effectiveness. Even CISOs of leading organizations concede that information security processes can often inadvertently interfere with business processes, which in turn affects threat intelligence and workflow analysis. To enlist employees as active participants in information security, companies need to alter the perception of security measures from one that views them as business impediments to one that embraces them as business enablers. Changing employee perceptions will translate into increased commitment at the operational level and, therefore, higher efficiency.

Ultimately the goal is to create a culture where employees serve as a source of information security intelligence and support. Communicating about information security policies in a way that relates directly to their work or personal lives can significantly increase the number of incidents reported by employees, as well as the quality of feedback provided by the business.

Moving Forward—Efficiently

In a business world where standing still could mean not just being outpaced, but being outdone, information security is more important than ever. Managing information security efficiently has become a business imperative.

The rapidly changing nature of threats and technologies has created the need for organizations to change their approach to information security management on a regular basis—including the five core dimensions of information security: strategy, organization, processes, technology, and culture. As Ragnar Schierholz, head of cybersecurity for the Process Automation Division at ABB, stated, "Information security is fast-changing, with new threat scenarios being developed constantly. Managers responsible for information security have to stay at the forefront of the latest developments to effectively and efficiently manage their risks."

> "You can have as many standards as you want, you can have as many technological checks, but awareness among the workforce remains critical."
>
> **— Vanessa Hanke, director of global security policy and standards, SAP**

In the context of efficiency, the central questions are "when to change and how much to change?" While being in the vanguard can be effective, it might not always be the most efficient way to proceed. The key is to make changes so as to stay one step ahead of cyber attackers. Adopting the measures described in this paper is a good first step.

The next step is to monitor, evaluate, and review the progress made with respect to each of the five dimensions of information security. By identifying key information security indicators tailored to their organizations, CISOs can objectively communicate the performance of the information security organization (similar to how a CFO presents financial performance indicators) to members of the board for review and assessment.

Organizations can start with indicators that are easy to measure and understand and that are limited to a representative set of functions, projects, and processes. These KSIs, when integrated into an actionable balanced scorecard, can help identify what and how much to change. The review cycle, as determined by the board in partnership with the information security team, will clarify when such changes need to be made. These KSIs can be linked to the business KPIs or to non-business KSIs (such as technical indicators about vulnerability management or patching). For example, an insurance company can map the KSI "percentage of incidents where customer data is put at risk" against the customer churn rate to create a measure of efficiency. Moving forward one step at a time, the company can introduce a set of

robust KSIs to address the effectiveness and efficiency of all information security-related issues. Having clearly defined goals and objectives can help the CISO and the information security team drive the change necessary to ensure that information security is successfully fending off attacks while reining in costs.

Creating an Immediate Impact

Success today is as much about having the right guidance as it is about having the right technology. When working with clients, we assist them by first assessing the current state and identifying gaps in the execution of information security (information security health check) and then developing a suitable information security strategy. While the information security health check focuses on effectiveness, the roadmap focuses on improving efficiency. Similarly, when working with clients to manage major information security programs, our goal is to identify more efficient ways to reach the company's business and security objectives—often using the rules discussed above.

Authors

Holger Röder, partner, Frankfurt
holger.roeder@atkearney.com

Dr. Boris Piwinger, consultant, Vienna
boris.piwinger@atkearney.com

This study was conducted in cooperation with the Mannheim Business School's full-time MBA program. The authors wish to thank the student team of Gourav Ghosh, Mina Kamal, Felix Kitschke, Manmeet Malhi, and Tina Su for their valuable field work, and offer further thanks to Gourav Ghosh, François Gratiolet, Russ Berkoff, and Mannheim Business School Prof. Dr. Armin Heinzl for their valuable inputs in writing this paper.

ATKearney

A.T. Kearney is a leading global management consulting firm with offices in more than 40 countries. Since 1926, we have been trusted advisors to the world's foremost organizations. A.T. Kearney is a partner-owned firm, committed to helping clients achieve immediate impact and growing advantage on their most mission-critical issues. For more information, visit www.atkearney.com.

Americas	Atlanta	Detroit	San Francisco
	Bogotá	Houston	São Paulo
	Calgary	Mexico City	Toronto
	Chicago	New York	Washington, D.C.
	Dallas	Palo Alto	
Asia Pacific	Bangkok	Melbourne	Singapore
	Beijing	Mumbai	Sydney
	Hong Kong	New Delhi	Taipei
	Jakarta	Seoul	Tokyo
	Kuala Lumpur	Shanghai	
Europe	Amsterdam	Istanbul	Oslo
	Berlin	Kiev	Paris
	Brussels	Lisbon	Prague
	Bucharest	Ljubljana	Rome
	Budapest	London	Stockholm
	Copenhagen	Madrid	Stuttgart
	Düsseldorf	Milan	Vienna
	Frankfurt	Moscow	Warsaw
	Helsinki	Munich	Zurich
Middle East and Africa	Abu Dhabi	Dubai	Manama
	Doha	Johannesburg	Riyadh

For more information, permission to reprint or translate this work, and all other correspondence, please email: insight@atkearney.com.

The signature of our namesake and founder, Andrew Thomas Kearney, on the cover of this document represents our pledge to live the values he instilled in our firm and uphold his commitment to ensuring "essential rightness" in all that we do.