Andrej Volchkov is the security program manager in the CSO office at Pictet, a private bank in Geneva Switzerland. Volchkov was previously in charge of security, compliance and internal solutions in Pictet's IT division and responsible for new technologies and architecture, IT methodologies, tooling, and software engineering. Volchkov has a wide range of experience that includes new technology and IT solutions implementation, management of multidisciplinary teams, project management, and software development and research.

How to Measure Security From a Governance Perspective

Good governance relies on reports or measures that either assess the adequacy of information security, the security program and the return on security investment (ROSI) or the progress toward fixed objectives.

Companies need a pragmatic approach for monitoring the effectiveness of security countermeasures to enable them to adjust their program accordingly and decide on investments. Presented here is an approach for establishing a security dashboard. It is aimed at executive management and provides responses to questions that might arise such as, "Is our security spending justified?" or "Is our security adequate?"

The term "monitoring" is used here to suggest the importance of tracking trends in relationship to precise measures. The term "security" is used rather than "information security," as it is possible to apply the same principles to all security domains including continuity, physical, and human or personal security.

JUSTIFYING SECURITY SPENDING

Security investment decisions are traditionally based on observations, a sense of vulnerability, threat assessments or audit findings. It is not uncommon to see a problem or incident trigger a project that aims to improve the posture or effectiveness of the countermeasures in place. Good governance, however, recommends that executive management be involved in strategic security decisions.[1] The more awareness of the importance of security metrics, or for better coordination of investment—beyond the simple technical IT problem to a concern for the company as whole—the greater the need to justify (i.e., explain) investment in security programs.

Questions such as "Is security spending adequate," or "How good is security?" are not only legitimate but are also part of a natural development toward better governance. The question of appropriateness of security[2] is crucial and is one of the major concerns in all good governance practice. This is precisely why measures need to be expressed in clearly defined units (e.g., hourly cost, incident, risk, budget, strategy) and accepted by all stakeholders in the company.[3]

Companies are increasingly being called on by external auditors who have been hired by their partners or clients to assess the level of security or compliance using norms or best practices. A standard approach to measuring or reporting security should contribute to reducing the cost of these repetitive audits.[4]

The need for justification is also accentuated by the fact that security officials are increasingly reporting to higher levels in companies and often outside of IT. According to a study by Forrester,[5] 54 percent of interviewed chief information security officers (CISOs) were reporting to a member of the C-suite in 2010; this is a 9 percent increase from the previous survey in 2009. The same study revealed that 42 percent of CISOs report outside IT. Similar findings are shown in "The 2011 Global State of Information Security Survey" by PricewaterhouseCoopers (**figure 1**).

Figure 1—CSO/CISO Reporting Level Progression

Percentage of chief information security officers or equivalent information security leaders who report to the followings senior executives:	2007	2008	2009	2010	Three-year % change*
Chief information officer (CIO)	38%	34%	32%	23%	-39%
Board of directors	21%	24%	28%	32%	+52%
Chief executive officer (CIO)	32%	34%	35%	36%	+13%
Chief financial officer (CFO)	11%	11%	13%	15%	+36%
Chief operating officer (COO)	9%	10%	12%	15%	+67%
Chief privacy officer (CPO)	8%	8%	14%	17%	+113%

Source: PricewaterhouseCoopers, "The 2011 Global State of Information Security Survey." Reprinted with permission.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

The ability to explain to management the strategy and purpose of security investments using appropriate business language and with a holistic perspective is essential. Senior management is, of course, ultimately responsible for security, which is why they request reports in the form of dashboards that contain stable key point indicators of how adequate the security is regarding the company's needs.[6]

Several surveys also indicate that it is becoming increasingly important to provide justification for investment in security because of the feeling that countermeasures already in place are inadequate. Threats evolve and security countermeasures (and investments) try to keep pace, albeit with a certain delay, but there is a sense of a never-ending race.[7]

WHY IT IS DIFFICULT TO MEASURE SECURITY

Merely observing incidents or studying statistics generated by technical devices does not enable us to form an opinion on the adequacy of security. How many incidents and what type of incidents are allowed in a good security setup? What happens if there are no incidents?

Security tools generate many traces of activity, such as patches applied, detected vulnerabilities, alerts, intrusion attempts, volume of mail processed by antivirus tools, authentication errors, traces of access to systems and changes in privileges. Log management tools can provide correlation of these traces and generate reports that ensure compliance with legal and regulatory requirements. However, high-level metrics require additional efforts to collate these different pieces of information.

Since the benefits (or economic value added [EVA]) of security investments are difficult to observe, why not try to estimate potential losses or annualized losses (annual loss expectancy [ALE]) in order to justify investments?[8] There are various formulas that prevent making investments that exceed the value of the assets under protection. One could also measure the total cost of ownership (TCO) of security and observe its evolution in relation to the estimate of potential losses. Several tools or methods are available to calculate the ROSI on the basis of analysis of losses and investments for specific processes.[9] The main difficulty with these methods stems from the fact that one has to associate the estimate of a loss with its likelihood of occurrence for all units under observation, which could be very random. One accurate calculation method requires statistics over several years with precise indicators on incidents, their nature and the associated expected losses.

Companies do not share their data or statistics on vulnerabilities and incidents because of the negative image that these statistics convey. There is no common definition or terminology that would allow an anonymous exchange on the basis of these statistics. The terms "incident," "attack," "loss" and "investment" mean different things to different companies.

Solution providers emphasize their ability to reduce costs with their solution and often present an associated model for calculating the ROSI for their solution. However, the security solutions sought by companies rarely focus on mitigating a single isolated risk. To optimize its investments, a company seeks comprehensive, flexible and often integrated solutions in suites of products that are usable for multiple purposes. As it is impossible to assign a solution to each specific risk, it becomes difficult to calculate the ROSI because of the side effects (positive or negative) on other risk factors and the ancillary costs associated with maintenance. The constant evolution of threats and the programmed obsolescence of technologies negatively impact a possible measurement program based on the individual components.

> "Being compliant with a standard does not mean having adequate security."

Being compliant with a standard does not mean having adequate security. Different standards (e.g., ISO 2700x, ISO 31000, ISO 38500, ISO/IEC 13335) or best practice guides (ITIL) can be used under certain conditions to assess security posture. However, these standards have stipulations regarding the existence of processes, but do not provide evaluation criteria. There are generally no recommendations about how to effectively manage and measure security.

MANAGERS WANT MEANINGFUL REPORTS

Managers are familiar with analyzing a company's high-level indicators—losses, gains, ratios, political and economic events, and sales targets—to make forecasts or to grasp a particular situation. Decision makers are less interested in operational metrics or calculations of return on investment (ROI) of a particular isolated security component, but rather are interested in reports on the overall efficiency of security countermeasures in place.[10] Because their concerns are revenue generation, cost reduction, improvement of products or services, and control of spending, security reports are appreciated only if they adopt the same approach and the same language (e.g., covering functional and strategic alignment, security performance objectives achievement, compliance management, security team performance, security added value for customers).

The strategy of investment in security has to target the mitigation of high risk areas and the improvement of less adequate or immature processes. For example, if the risk report highlights a significant risk on information leaks and, at the same time, the data access control process is considered immature, it is necessary to implement a data protection solution (such as encryption, improvement of access rights or a data leak prevention tool).

An executive management report should, therefore, contain at minimum the following three sections:

- Explanation of a strategy and security program
- Operational efficiency of a security organization
- Cost of security deliveries

TOOLS TO ASSESS THE STATE OF SECURITY

There are four common tools that each CSO/CISO can use to demonstrate the added value of a security program:

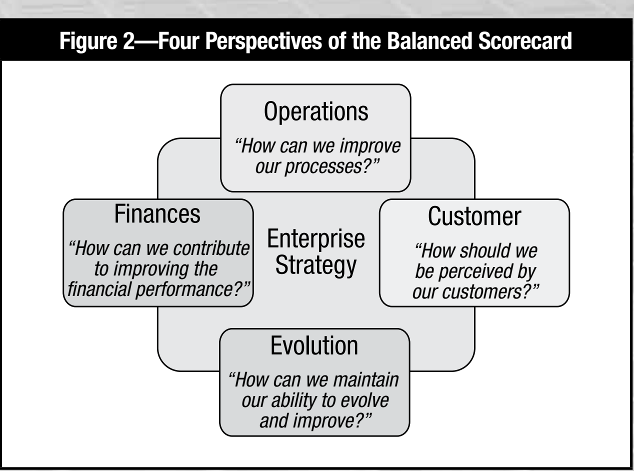
1. Security balanced scorecard
2. Risk management
3. Maturity modeling
4. Diagnostic (or goal-question-metric) method

Security Balanced Scorecard

The balanced scorecard (BSC) is a widespread method for monitoring performance and progress toward the goals fixed to endorse the enterprise's strategy.[11] This tool is well known to management, and it enables security teams to communicate findings on a formal basis. If it is used for monitoring security performance, it will help to position the security team as a partner to the other business lines, making its contribution part of a joint effort. The use of a BSC stimulates executive management into taking ownership of security issues and security's added value.

Financial performance measures alone do not convey all the information needed to assess the contribution of different activities. In addition to finance-related measures, the BSC approach requires measures on three other dimensions or perspectives: operations, customer relationships and evolution (or learning and growth). The four perspectives must contribute to the support of the strategy and the vision of the company. One main question can be associated with each perspective to guide the user in the choice of objectives and associated metrics (**figure 2**).

Figure 2—Four Perspectives of the Balanced Scorecard


Operations
"How can we improve our processes?"
Finances
"How can we contribute to improving the financial performance?"
Enterprise Strategy
Customer
"How should we be perceived by our customers?"
Evolution
"How can we maintain our ability to evolve and improve?"

The number of objectives should be limited and the number of metrics per objective should be restricted to three or four. The BSC method can also be used for part of the organization or for a specific security domain (e.g., to monitor the business continuity objectives in a company branch or subsidiary).

The BSC-based report has four chapters—each connected with one perspective. Each chapter should contain the objectives to be achieved and the associated metrics. Some examples of objectives with associated metrics are shown in **figure 3**.

Security Risk Management

The aim of investing in security is to mitigate or prevent risk to property or corporate assets. The definition of risk and especially the assessment of risk are essential indicators for high-level management decision making.

Figure 3—Examples of Metrics in Security Balanced Scorecard

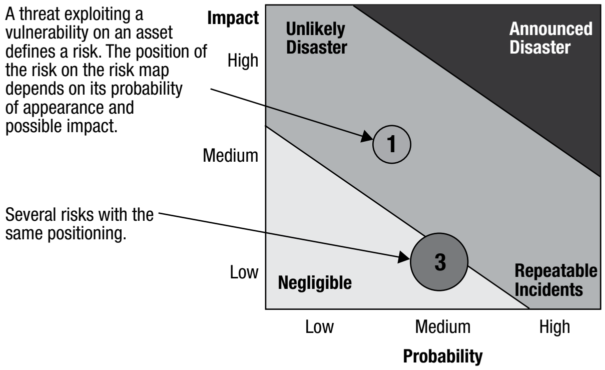
Perspective	Objectives	Metrics
Finance	• Manage the cost of security.	• Security total cost of ownership (TCO) vs. number of employees (ratio) • Cost of security incident resolution
	• Improve the efficiency of the information leak controls.	• Number of checks conducted vs. number of employees (ratio) • Percentage of emails covered by controls vs. number of employees (ratio)
Operations	• Reduce the risk of information leakage by negligence.	• Intrusion detection tests • Number of rule breach findings
	• Reduce the number of exceptions and special permissions for mobile workers.	• Number of exceptions per year
	• Improve the access rights management process.	• Number of changes in privileges vs. number of employees (ratio)
Customer	• Reduce the error rate in granting access rights to customers.	• Error rate in the process of granting of access rights • Number of help-desk calls on security issues
	• Reduce by 50 percent the delay in allocating new access rights.	• Delays in assignments of access rights
	• Reduce the delay in processing end-user requests.	• Average delay
Evolution	• Increase the level of understanding of end-user security issues.	• Cost of awareness program vs. number of employees
	• Review the security policy according to the needs of the business.	• Result of the survey conducted in the business lines

A security risk can generally be identified through threats that are likely to exploit one or more vulnerabilities on the company's assets. For example, the risk of penetration of a company's computer network is present because of threats such as intrusion attempts that exploit various vulnerabilities, e.g., social engineering.

The risk is then evaluated on two dimensions, namely the probability of its occurrence and its impact. It is then positioned on a risk assessment matrix (**figure 4**). There are several possibilities for expressing the probability (e.g., frequency of occurrence) and impact (i.e., financial, reputational, human, other).

Probability and impact assessments are based on the same indicators as those used to measure threats and vulnerability. As noted previously, it is impossible to calculate these accurately. It can, however, be roughly evaluated as low, medium or high, using knowledge, statistics, and other endogenous and exogenous factors, which, generally speaking, should be enough to position a risk. In some cases the company may also appoint external experts to assess a specific risk (e.g., penetration test).

Figure 4—Risk Assessment Matrix


A threat exploiting a vulnerability on an asset defines a risk. The position of the risk on the risk map depends on its probability of appearance and possible impact.
Several risks with the same positioning.
Impact
High
Medium
Low
Unlikely Disaster
Announced Disaster
1
3
Negligible
Repeatable Incidents
Low
Medium
High
Probability

Maturity Modeling for Information Security

The risk management process provides information on the dangers, but does not show the level of preparation or the security posture. Therefore, the security process maturity should be evaluated so that initiatives can be prioritized and aimed at addressing weaknesses.

Figure 5—Example of Criteria for Assessing the Degree of Compliance to Point 5.1 of ISO 27002

	Section	Evaluation criteria 0: Incomplete 1: Performed 2: Managed 3: Established 4: Predictable 5: Optimized	Current Level	Desired Level
5	Security Policy			
5.1	Information Security Policy	0: There is no documented security policy. 1: The security policy applies to certain departments or units in the organization. 2: Security policy is documented and addresses all areas. 3: Security policy defines the responibilities and sets the framework for all lines of business. The documentation is compiled. 4: Security policy and the associated documentation are reviewed regularly. The policy is adapted for the needs of all business lines. 5: Each employee knows the security policy. The organization regularly adapts the policy, the directives and associated documentation.	2	3

Standards such as ISO 2700x can be used as a reference to build a maturity model. However, these standards recommend the use of a practice, but they do not stipulate any criteria for assessing the level of compliance. For example, point 5.1 of the ISO 27002 standard calls for the existence of a security policy, but it does not specify any gradation that can be found in practice such as "the formal policy does not exist or is not known," or "the policy exists, but is not revised" or "the policy exists and is revised regularly."

To use standards in the maturity assessment process effectively, evaluation criteria must be created for each point of the standard. For this purpose, one could adopt ISO 15504 standard criteria and then establish evaluation criteria for each chapter of the ISO 27002 standard (see **figure 5**).

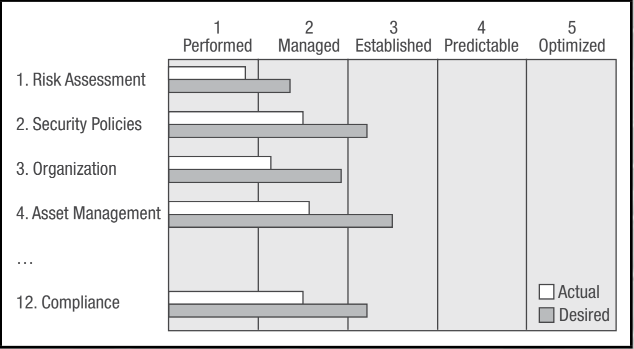
Each maturity model consists of a questionnaire covering all the chapters of one or more standards or frameworks (e.g., ISO 2700x, COBIT, NIST) or proposing its own catalog of measures. Therefore, the current level of maturity for each chapter of the standard should be assessed according to the proposed criteria alongside the desired level. The tool then calculates the averages for each section of the standard or another grouping (possibly weighted measurement) and shows a chart of the state of maturity (**figure 6**).

There are several tools or methods available to measure maturity, such as The Open Group Maturity Model for Information Security Management.[12] Large consulting firms also propose their own models and tools for security maturity assessment, such as Forrester's Information Security Maturity Model.[13]

A maturity model can be used as a tool to communicate security posture to different stakeholders. It also facilitates explanation of the initiatives contained in the security program: *why* information is essential, especially for teams tasked with developing countermeasures, such as IT.

The scope of maturity assessment may be limited for both the business sector and the domains of the model. For example, the maturity of security management at a company's subsidiary can be assessed. Furthermore, the assessment of maturity and the risk assessment are opportunities to discuss and compare views about security with the business representatives, risk managers, auditors and any other stakeholders.

Figure 6—Representation of Maturity: Actual and Desired



The Common Criteria (ISO/CEI 15408) is a standard for security evaluation and certification of a specific system or product. The system certified at one level satisfies all criteria from precedent levels as well as those at the certification level. A similar approach is suggested in the method of measurement of resilience of the Software Engineering Institute (SEI).[14] It evaluates resilience (continuity and IT operations) using the Capability Maturity Model Integration (CMMI) criteria. The resilience is certified as being at a certain level if it meets the requirements of that level as well as requirements from the previous level.

Figure 7—Metrics Associated With a Hypothesis

Hypothesis	Subhypothesis	Metric
The management of access rights is no longer appropriate.	Delays in the allocation of access rights increase.	Average delay in a period of time
	Inappropriate access rights increase.	Number of post corrections vs. number of change requests
	The complexity increases (which negatively impacts the risk of error).	Number of different IT systems vs. number of post corrections

Diagnostic Method

The proverb “you cannot improve what you cannot measure” can be adjusted to “you cannot measure if you do not know why you are measuring.” Setting goals prior to measuring facilitates the choice of metrics. One of the main purposes of these measurements is to demonstrate a trend or prove a hypothesis.

One strategy is to simplify the definition of metrics, subdivide the hypothesis into subhypotheses or questions, and then define metrics related to each question. One example of the subdivision of a hypothesis and associated metrics is shown in **figure 7**.

The process for constructing this measurement plan is the following:

1. **Determine the hypothesis and goal**—The hypothesis is: The access rights process in an organization is no longer appropriate. The goal would be to improve it according to the result of measuring.
2. **Subdivide into questions or subhypotheses**—The questions associated with the hypothesis or goal are:
   - What are the delays in allocation of access rights? The subhypothesis is that they increase.
   - Is there a progression of errors? The subhypothesis is that incidents or inappropriate access rights increase.
   - Is the complexity of the IT system correlated to the increase in number of errors? The subhypothesis is that the more complex the system, the more errors there are.
3. **Determine the metrics**—The metrics associated with the previous questions could be the following:
   - Average delay (elapsed time between the change request and the availability of the new access rights) measured during a set period of time (e.g., last three months)
   - Ratio between the number of post corrections and number of change requests
   - Evolution over a period of time of the ratio between the number of different IT systems and the number of post corrections

There are different methods of measuring by objective, such as the Diagnostic Method from McKinsey[15] or the Goal-Question-Metric (GQM).[16] The process described for designing metrics is beneficial because it is simple, bounded to the initial hypothesis or goal, and constructed top-down.

EXAMPLE SECURITY DASHBOARD

The ultimate goal of every measurement action is to present a dashboard, a report or a summary of the state of security and associated trends. The following example of a dashboard contains the highlights of measures that respond to issues that can arise in each of the following areas:

1. **Strategy and security program**—What is the security strategy and program?
2. **Operational performance**—How is operational performance changing? What are the main tasks and responsibilities of a security team?
3. **Monitoring the objectives**—Were the agreed-upon objectives achieved?
4. **Costs**—How are security costs distributed?

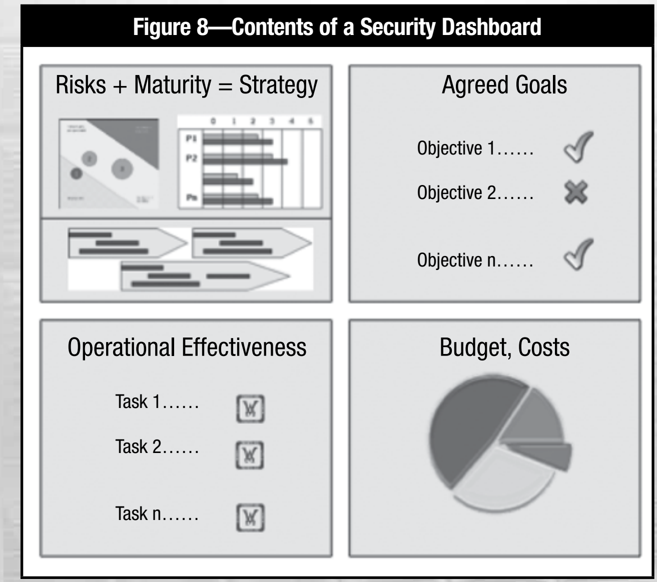
The high-level content of such a dashboard is shown in **figure 8**. It is important that all indicators and metrics used for the report are made available. This helps clarify the conclusions conveyed by the diagrams and tables and answer any additional questions.

Strategy and Security Program

A security program consists of all the initiatives for a given period (usually one year). It contains projects and other activities—all of which are aimed at mitigating high risk factors or increasing a company’s ability to protect its assets. It is sometimes called a business plan or investment plan.

The risk assessment and maturity model are two dimensions of the corporate security posture. Any initiative (e.g., IT projects, policy or guideline changes, awareness campaign, acquisition of products) can be viable only if it targets mitigation of risk and/or improvement of one or more immature security processes.

Figure 8—Contents of a Security Dashboard



Presentation in a dashboard or annual reporting can take different forms. The three main elements—risk, maturity and strategy—can be presented on a single page, with particular focus on important risk areas or critical processes that need improvement.

Operational Performance and Cost

Operational performance must be presented using numbers, ratios and trends. **Figure 9** shows examples of operational metrics. Again, these metrics should be chosen according to the measurement objectives and should cover a specific period of time to illustrate the trend. Security costs should be presented alongside the deliverables of a security team.

Follow-up on the Objectives

Security countermeasures should be implemented to overcome the weaknesses identified by the audit findings, maturity assessments or risk analysis. All these objectives should be well defined. The results can be presented in the form of a security balanced scorecard (**figure 10**).

CONCLUSION

Establishing a method for measuring or monitoring security is a necessity in order to meet the demands for justifying an organization's security investments. Security is no longer an obscure and technical area left to the whim of a few specialists. Modern governance standards require executive managers to have a vision of, and development strategy for, security.

It would be a mistake to imagine that one can accurately measure ROSI for a whole security system in one organization. It is wiser to try to answer security-related questions raised by executive managers in a language that they can understand, using tried and tested methods and tools, such as a balanced scorecard, maturity models and risk management.

Security dashboards are a good way of presenting and monitoring security from a governance perspective. They must contain a succinct explanation of the security strategy and

Figure 9—Examples of Operational Efficiency Metrics

Deliveries of a Team	Metric	Efficiency Trend	Cost	Cost Trend
Awareness efforts	• Cost of awareness program vs. number of security incidents due to poor awareness (ratio)	↓	$	↓
Compliance strengthening	• Average delays in improvements according to audit findings • Number of systems in compliance vs. number of systems to be made compliant (ratio)	↑	$	→
Incidents processed	• Number of security incidents vs. number of employees (ratio)	↑	$	→
Unavailability rate of security components	• Number of hours of unavailability vs. number of components (ratio)	→	$	→
Efforts to ensure that IT projects are compliant	• Number of employees devoted to security projects vs. total cost of complex projects (with high security impact) (ratio)	↑	$	→
Effectiveness of identity management	• Number of accounts still open after end users leave • Number of changes in privileges • Total number of different systems and applications under management • Average delay in processing requests • Error rate	↑	$	↑
Efforts in processing alerts and other security events	• Number of specific investigations • Number of working days spent on analyses vs. number of employees (ratio)	↑	$	→
Effectiveness of controls	• Checks carried out vs. number of employees (possibly by nature of checks or severity of checks) (ratio) • Number of breaches vs. checks carried out (possibly by nature or severity of controls) (ratio)	↓	$	→

Figure 10—Security Balanced Scorecard Example

	Objective	Measure	Result
Operations	Improve controls of outgoing emails.	Success in implementing automatic control is achieved.	X
	Reduce security constraints for business.	Help-desk calls regarding security are reduced by 10 percent.	✔
	Be more efficient in the audit findings implementation.	Ninety percent or more of improvements according to audit findings are done on time and on budget.	✔
Customers	Decrease the delay in processing the application of customer access rights.	Delay is reduced to a maximum of one day.	X
Evolution	Reduce the risk of intrusion by email.	Intrusion tests using social engineering is sufficient after sensitizing staff. Target: no more than 5 percent successful intrusions	✔
	Involve security representatives when business-line security directives are drawn up.	More than 50 percent of security representatives have suggested directives.	✔
Finance	Minimize the gap between security budget and actual spending.	The difference between budget and expenditure does not exceed 10 percent.	✔

program, different operational trends based on indicators and metrics, a summary of the progress toward agreed-upon goals, and a presentation of security costs.

ENDNOTES

[1] IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, USA, 2006, *www.isaca.org*

[2] Allen, Julia; "Governing for Enterprise Security," Carnegie Mellon University, USA, 2005

[3] Gartner, "Avoid Inappropriate Financial Justifications of Security Expenditures," 11 July 2007, *www.gartner.com/id=509685*

[4] Ferrara, Ed; "Develop Effective Security Metrics," Forrester Research Inc., USA, 17 January 2012, *www.forrester.com/Develop+Effective+Security+Metrics/fulltext/-/E-RES45787?objectid=RES45787*

[5] Ferrara, Ed; "Don't Bore Your Executives—Speak to Them in a Language They Understand," Forrester Research Inc., 18 July 2011, *www.forrester.com/Develop+Effective+Security+Metrics/fulltext/-/E-RES45787?objectid=RES45787#/Dont+Bore+Your+Executives+8212+Speak+To+Them+In+A+Language+That+They+Understand/quickscan/-/E-RES58885*

[6] Slater, Derek; "Security Metrics: Critical Issues," *CSO Online*, 2012, *www.csoonline.com/article/455463/security-metrics-critical-issues*

[7] Brenner, Bill; "Companies on IT Security Spending: Where's the ROI?," *CSO* Online, 25 January 2010, *www.csoonline.com/article/518764/companies-on-it-security-spending-where-s-the-roi-*

[8] Fitzgerald, Michael; "Security and Business: Financial Basics," *CSO Online*, 23 June 2008, *www.csoonline.com/article/394963/security-and-business-financial-basics?page=1*

[9] Berinato, Scott; "A Few Good Information Security Metrics," *CSO Online*, 1 July 2005, *www.csoonline.com/article/220462/a-few-good-information-security-metrics*

[10] Rosenquis, Matthew; "Measuring the Return on IT Security Investments," Intel, 2007, *http://communities.intel.com/docs/DOC-1279*

[11] Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business Review Press, USA, 1996

[12] The Open Group, "The Open Group Releases Maturity Model for Information Security Management," press release, 2011, *www.opengroup.org/news/press/open-group-releases-maturity-model-information-security-management*

[13] Forrester, "Assess Your Security Program With Forrester's Information Security Maturity Model," 2013, *www.forrester.com/Assess+Your+Security+Program+With+Forresters+Information+Security+Maturity+Model/fulltext/-/E-RES56671*

[14] Allen, Julia H.; Pamela D. Curtis; "Measures for Managing Operational Resilience," Carnegie Mellon University, USA, 2011

[15] Jaquith, Andrew; *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, USA, 2007

[16] Hayden, Lance; *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*, McGraw Hill, USA, 2010