Security Effectiveness Framework Study

Is your organisation effective in managing its security operations?

Sponsored by:
HP Information Security, and
Check Point Software Technologies Ltd.

31 July 2010
Introduction
About the Security Effectiveness Framework Study

HP Information Security, and Check Point Software Technologies Ltd. in partnership with Ponemon Institute, recently conducted the Security Effectiveness Framework Study. The aim was to learn what IT security leaders in more than 100 UK and European companies think are the key components to having an effective security operation that helps to deliver a measurable impact on business performance and add value while protecting an organisation’s information assets and critical infrastructure. Vistorm and Check Point are using the findings to help security leaders align their activities with business goals and focus on the areas needed to manage their operations more effectively.

HP Information Security has a history of pioneering solutions that deliver effective and measurable reduction in organizational risk, lower long term investment in information security, and improved security posture. While other providers lock down information to protect it, our success is driven by viewing information security differently.

HP Information Security experts take a proactive, risk based approach—Dynamic Information Security—ensuring freedom of information to those who should have access while enabling new opportunities. We structure a strategic, end to end approach around the four most critical areas of the information security lifecycle: Security Strategy, Security Programmes, Security Operations and Security Assurance. We engage with our clients at different stages and help them to move through the cycle—from initial risk reviews through to full security transformation.

HP Information Security delivers a complete security capability, HP Secure Advantage, and unique toolsets, including the Information Assurance platform and security analytics from our business-ready Security Innovation program with HP Labs. These toolsets are all focused on delivering an effective reduction in risk for the world’s most successful public and private organizations.

Check Point Software Technologies Ltd. the worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to innovate with the development of the Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be fully customised to meet the exact security needs of any organisation or environment. Check Point customers include tens of thousands of businesses and organisations of all sizes including all Fortune 100 companies. Check Point’s award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

The Ponemon Institute is dedicated to advancing responsible information management practices that positively affect privacy, data protection, and information security in business and government. The Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organisations.

The Institute has assembled more than 60 leading multinational corporations called the RIM Council, which focuses the development and execution of ethical principles for the collection and use of personal data about people and households. The majority of active participants are privacy or information security leaders.
Highlights

101 organisations participated in this study. Of those, 35% had a security effectiveness score (SES) below the study average, indicating that they are not performing as effectively as others above the average SES.

The biggest barrier to effectiveness, according to the majority of respondents, is a sufficient budget to accomplish the following:

- Achieve its mission and objectives.
- Ensure IT systems are not disrupted or brought down by attackers.
- Achieve certification from reputable authorities such as ISO, NIST, PCI and others.
- Curtail or minimise data breach incidents.
- Ensure policies are strictly enforced throughout the enterprise.

Based on the SES, organisations are most effective at doing the following:

- Performing timely updates for all major security patches.
- Limiting physical access to data storage devices containing sensitive or confidential information.
- Complying with legal requirements and policy laws and statutes.
- Aligning security programmes with self-regulatory requirements such as ISO, NIST PCI and others.

The main barriers to effectiveness are:

- Being able to make the business case and demonstrate the tangible benefits of the company’s IT security program. As shown above, the majority do not have the budget or resources to be as effective as possible.
- Being able to prevent or curtail cyber attacks, including advance persistent threats.
- Sixty-three percent do not believe their security budget is sufficient to curtail or minimise data breach incidents.
- Prevent or curtail viruses and malware infections.

The effectiveness metrics that have the greatest impact on security effectiveness are policy enforcement (22%) and compliance (20%) - see Pie Chart 3, Effectiveness metrics.

The input variables that have the most impact are security environment (22%) and governance (21%) - see Pie Chart 2.

Top 5 drivers to a good Security Effectiveness Rating

- Appointment of a CISO or organisational leader for information security.
- Training and awareness programs on data protection and security for end-users.
- An organisational culture that respects privacy and data protection.
- Executive-level support for security.
- Strong endpoint controls.

Top 5 consequences of a poor Security Effectiveness Rating

- Inability to achieve a high security posture.
- Insufficient budget or resources.
- Lack of strong perimeter controls.
- Inability to attract and retain credentialed or experienced staff.
- A security strategy that is not consistent throughout the enterprise.
Executive overview

Security effectiveness impacts business performance and operational success

Forrester (2009) reports that organisations are spending 11.2% of IT budget on security. Security's growing importance is also reflected in the fact that some 44% of companies now employ a CISO (2010 PricewaterhouseCoopers survey) Security is a massive cost to any business and, as with any cost, this needs to be justified and show a measurable Return on Investment.

Successful organisations understand that a good security posture helps them to improve competitiveness and profitability through reduced business and financial risk and better protection of their data and corporate reputation. However, security leaders face the challenge of managing increasing threat levels and dealing with continuing budget pressures while security costs continue to rise. Many are also restricted by the fact that budgets are outside their control with stakeholders focused on revenue growth, operational efficiency, IT effectiveness and cost reduction. Security leaders are also frequently dependent on the IT department to deploy the solutions they need.

Although the need for greater security effectiveness is widely acknowledged, the problem has been to find a satisfactory method of identifying and measuring any improvements to create a more effective department. Any approach must deliver business outcomes while taking account of the impact and interdependence of people, processes, culture, technology and controls.

The aim is to create an effective security operation that allocates the appropriate budget and resources to achieve the organisation’s desired level of security and protection of sensitive and confidential information, based on its accepted level of risk, while causing minimal disruption to the business. The goal is to enable an organisation to apply the right level of resources to achieve the desired security for its operations, while minimising any waste of resources.

Vistorm, Check Point and the Ponemon Institute carried out an independent study with more than 100 security leaders of some of the most successful companies in the UK and Europe. This study identifies the critical factors that affect security effectiveness and provides a summary of industry views on the relative importance of those factors. The findings provide the basis for a measurement tool – the Security Effectiveness Framework - that security executives can use to compare their own performance against a set of metrics that help to define a new standard for managing security. They can also compare their results to those of their peers and the sample group as a whole.

This tool will help security executives to identify priorities for improving performance and productivity in the most critical areas. It will also provide a measurable basis for building the business case and calculating Return on Investment for funding improvements. This process will, in turn, help to elevate information security to a board-level decision by demonstrating the alignment of security with business objectives and providing measurable business outcomes.

“Organisations that have achieved a high level of security effectiveness are better able to identify major data breaches, secure confidential information, limit physical access to data storage devices and achieve compliance with legal and self-regulatory frameworks. They are also in a better position to attract and retain high-quality security personnel and enforce corporate policies.”

Martin Sadler – Director of Security, HP Labs
The Security Effectiveness Framework

An effective security operation is one that allocates the appropriate budget and resources to achieve the organisation’s desired level of security and protection of sensitive and confidential information, based on its accepted level of risk, while causing minimal disruption to the business.

The Security Effectiveness Framework, developed by the Ponemon Institute, is a tool that measures the security of an organisation based on its current security posture. Security experts use the input from the tool to generate a Security Effectiveness Rating (SER) and provide a detailed report that enables security leaders to measure their effectiveness against six dimensions.

Dimensions of effectiveness

Security experts have identified the following six metrics as critical to achieving security effectiveness:

- **Uptime**: The ability to withstand cyber attacks and avoid costly business disruption.
- **Compliance**: The ability to achieve compliance with all applicable regulations and laws.
- **Threat containment**: The ability to prevent or quickly detect external security threats such as cyber crime, social engineering or malicious attacks.
- **Cost management**: The ability to manage investments in information security and data.
- **Breach prevention**: The ability to prevent or quickly detect internal security threats such as the negligent or incompetent insider.
- **Policy enforcement**: The ability to monitor and strictly enforce compliance with internal policies, procedures and other security requirements.

Business impact of security effectiveness

- **Uptime** - Respondents to the study recognise that business interruption resulting from cyber attacks significantly impact the productivity of IT and end users throughout the organisation. That’s because organisations must be able to deliver information services to employees, customers and partners when they need it and how they need it. Denial of service attacks can affect this directly, as do over-restrictive security policies that can halt or slow the delivery of information. If systems fail, it can also impact revenue as well as the productivity of IT and the end user. For example, if a major online retailer like eBay has a system failure it can cost that company around $2,000 per second in lost revenue.

- **Compliance** - An important part of the security mission within most organisations concerns compliance with best practices and standards such as ISO, NIST, PCI DSS and many others. Failure to comply with these requirements diminishes the organisation’s ability to reduce security risks and prevent cyber crimes. Compliance failure can also lead to fines and loss of business through damage to the corporate reputation. Compliance gives an independent perspective on how well an organisation is performing its information security duties. However, it should not be used as the model for delivery of information security services, but more a series of checks to identify improvement.

- **Threat containment** - Threat containment is an important element of corporate risk management, identifying the threats or risks to the business and then reducing or mitigating any damage the threat may cause. Ponemon Institute’s recently-published Cost of Cyber Crime’ study shows that the inability to quickly contain a cyber crime substantially increases the total economic impact to the organisation. Respondents to the study confirmed the fact that threat containment is essential to achieving an effective and efficient security posture.

- **Cost management** - Ponemon Institute research has repeatedly shown that organisations spend an insufficient amount of resources to reduce security risks and to enhance security posture. Cost efficiency in this context means that the security leadership of an organisation spends limited resources in ways that bring about the greatest benefits. The aim is to ensure efficient use and maximum value from available resources. As well as managing costs down to stop security costs spiralling out of control year by year, cost efficiency should also focus on improving ROI and achieving tighter control of delivery.
Security Effectiveness Framework study

- **Breach prevention** - This is a progressive and preventative series of processes and checks that aim to reduce the opportunity and impact of breaches in security policy and infrastructure. Ponemon Institute has studied the organisational cost associated with the loss or theft of confidential or sensitive information such as employee records, customer information and consumer data. This research shows that an organisation must mitigate or substantially reduce the leakage of the above-mentioned data categories in order to achieve compliance with leading regulators such as the ICO and the European Privacy Directive. Ponemon Institute has empirically determined the cost of a data breach for UK organisations at £67 per record. This number does not include substantial fines such as the ICO mandated £500,000 for organisations that are grossly negligent in their responsibility to protect data.

- **Policy enforcement** - Respondents to the study fully acknowledge that employee adherence to security requirements is essential to achieving a culture of good security, privacy and data protection. Organisations that fail to enforce compliance tend to diminish the importance of security and other related control objectives. The security policy is the embodiment of an organisation’s approach to information security. Enforcement is about both checking that the policy is understood and followed, but also that it can be translated into operations, as well as day-to-day activities, procedures and roles. Each part of an organisation must understand the relevance and impact of the corporate security policy on their function and role.

**Rating security effectiveness**

A high rating against each metric indicates that an organisation’s security efforts are meeting its objectives. A low rating indicates the opposite and highlights a need for improvement.

To provide further practical insight into areas for improvement, the results from the tool enable security leaders to relate their effectiveness to the level of five key resources that are available to them:

- Adequacy of the budget.
- Specific technologies deployed.
- Specific control activities conducted.
- Specific security governance practices.
- Organisational culture.

Security leaders can use results of the tool to determine whether they are achieving the highest level of effectiveness for a given level of resources. The results are also compared against industry groups and the database as a whole.

**What security leaders think**

While there are clear strategic and operational benefits in improving security effectiveness, it was essential to empirically validate the key components of an effective and efficient security operation. More than 100 highly-experienced security leaders provided survey feedback to validate the Security Effectiveness Framework tool.

Analysis of the survey findings reveals that there is a general consistency in the way security leaders frame effectiveness in the domain of information security and data protection. According to the organisations in the study, the key drivers to better effectiveness are technologies, control practices and governance. They also see the importance of organisational culture and budget in driving improvements.

**Top 5 drivers to a good Security Effectiveness Rating**

- Appointment of a CISO or organisational leader for information security.
- Training and awareness programs on data protection and security for end-users.
- An organisational culture that respects privacy and data protection.
- Executive-level support for security.
- Strong endpoint controls.

**Top 5 consequences of a poor Security Effectiveness Rating**

- Inability to achieve a high security posture.
- Insufficient budget or resources.
- Lack of strong perimeter controls.
- Inability to attract and retain credentialed or experienced staff.
- A security strategy that is not consistent throughout the enterprise.

**Improving information security effectiveness**

Improving security effectiveness can make an important contribution to organisational success. Vistorm and Check Point can help security leaders improve effectiveness by working in partnership to optimise existing resources and identify strategies and solutions.

Using the Security Effectiveness Framework tool, experts from Vistorm and Check Point take users through a series of questions covering adequacy of the budget, specific technologies and control activities deployed or not deployed, security governance practices and organisational variables. The responses are used to calculate a Security Effectiveness Rating and a report that highlights priorities for improvement and provides a firm basis for decision making and investment planning.

---

Part 1

Security Effectiveness Benchmark Study Results
Results – of the Security Effectiveness Framework Study

The Security Effectiveness Framework Study focuses on operational effectiveness in the information security environment for a sample of 101 UK and European organisations. The purpose of this research was to develop and empirically validate the Security Effectiveness Framework in terms of an organisation’s current security posture, key variables and output metrics which are shown in Figure 1. This figure provides a simple diagram of the framework, with operational effectiveness defined by key inputs and moderating variables – resulting in the six output metrics for success described in the executive overview:

- **Uptime:** The ability to withstand cyber attacks and avoid costly business disruption.
- **Compliance:** The ability to achieve compliance with all applicable regulations and laws.
- **Threat containment:** The ability to prevent or quickly detect external security threats such as cyber crime, social engineering or malicious attacks.
- **Cost efficiency:** The ability to manage investments in information security and data protection in a competent (non-wasteful) manner.
- **Data breach prevention:** The ability to prevent or quickly detect internal security threats such as the negligent or incompetent insider.
- **Policy enforcement:** The ability to monitor and strictly enforce compliance with internal policies, procedures and other security requirements.

![Figure 1: Schema of the security effectiveness Framework](image)

Inputs

- Technology
- Operations*
- Governance
- Budget

Moderating variables

- Industry
- Regulatory
- Culture
- Security effectiveness
- Economic health
- Global footprint

Security effectiveness metrics

- Uptime
- Compliance
- Threat containment
- Cost efficiency
- Breach prevention
- Policy enforcement

*Operations include staffing, training and control practices
The inputs are an organisation’s security technology, operations, governance and budget. Organisational characteristics (moderating variables) have been shown to influence the effectiveness of a security function. For example, perceptions that trust is important can support an organisational culture that respects privacy and data protection. Strategic organisations are more likely to believe in the importance of having a CISO or high-level security professional as someone to lead the security initiatives. The result of these inputs and organisational variables are six security effectiveness metrics as described in Figure 1.

The first part of the survey is used to determine how respondents perceive their organisation. As shown in Figure 2, the majority say that their organisation can be characterised as trusted and not risk averse. Less than half believe their organisation is efficient, strategic and innovative.

The second part of the benchmark survey instrument asks questions about the security environment in their organisations. The survey consists of separate statements that define reasonable security practices according to trusted certification authorities such as ISO, NIST and others. Respondents were asked to rate their organisation’s ability to achieve one of 13 specific security objectives. Our rating uses a confidence scale from “very confident” that the organisation accomplishes a particular security objective to “not able to accomplish.”

Responses to the 13 items are then scored from a +2 for a very confident response to -2 for not able to accomplish response. The average of all 13 questions defines the security effectiveness score (SES) for the respondent’s organisation. This average from all respondents is used in the research as a surrogate for security effectiveness, which is one of the moderating variables shown in Figure 1.

Figure 3 reports the distribution of the SES for 101 organisations in ascending order. As can be seen, the average SES for the present sample is .08. The highest SES is 1.9 and the lowest SES is -1.8.

Table 1 provides the aggregated average rating for the present sample of 101 respondents. The computation for each item is simply a weighted average (where 2 points are assigned for a very confident response, 1 for a confident response, -1 for a not confident response and -2 for unable to accomplish response).1

<table>
<thead>
<tr>
<th>Trust</th>
<th>Risk taking</th>
<th>Efficient</th>
<th>Strategic</th>
<th>Innovative</th>
</tr>
</thead>
<tbody>
<tr>
<td>52%</td>
<td>50%</td>
<td>47%</td>
<td>45%</td>
<td>43%</td>
</tr>
</tbody>
</table>

1 Ponemon Institute developed the SES methodology in partnership with PGP Corporation. It was first used in the 2005 Encryption Trends Study. Since then, the SES has been used in more than 50 Ponemon Institute studies.
As shown in Table 1, respondents believe their organisations are most effective at performing timely updates for all major security patches, limiting physical access to data storage devices containing sensitive or confidential information, and complying with legal requirements and policies including privacy laws and statutes. Least effective are ensuring third parties have adequate security practices, preventing or curtailing cyber attacks including advanced persistent threats and preventing or curtailing viruses and malware infections.

Ponemon Institute developed the SES methodology in partnership with PGP Corporation. It was first used in the 2005 Encryption Trends Study. Since then, the SES has been used in more than 50 Ponemon Institute studies.
Culture supports security effectiveness

Figure 4 compares SES results to five organisational characteristics. As shown, organisations in the study with the most favourable perceptions about their culture have a higher security effectiveness score.

The organisations in the study are grouped into four quartiles according to their SES scores. Comparing average SES for the first and fourth quartile results for each one of the five organisational characteristics, it is clear that favourable ratings about organisational characteristics (Quartile 1) correspond with higher SES and unfavourable ratings (Quartile 4) correspond to a lower SES rating. Organisations perceived to be trusted and efficient have the highest SES. Similarly, those with unfavourable views tend to have a lower SES.

Figure 5 compares all four quartile results, again showing that ratings about organisational characteristics are systematically related to SES scores. Specifically, respondents who hold a more favourable impression about their companies also enjoy higher SES results.

Budget influences security effectiveness

Six attributions about the respondents’ security budget are summarised in Table 2. The combined average of the strongly agree and agree rating is 40 percent, and less than 50 percent in five of six statements. This suggests that respondents hold a net unfavourable perception about the adequacy of their organisation’s security budget.

Table 2: Respondents’ perceptions about the adequacy of the security budget

<table>
<thead>
<tr>
<th>Q#</th>
<th>Attributions about your organisation’s budget</th>
<th>Strongly agree</th>
<th>Agree</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>My organisation’s security budget is sufficient to accomplish its mission and objectives.</td>
<td>14%</td>
<td>24%</td>
<td>38%</td>
</tr>
<tr>
<td>2</td>
<td>My organisation’s security budget is sufficient to ensure our IT systems are not disrupted or brought down by attackers.</td>
<td>13%</td>
<td>25%</td>
<td>39%</td>
</tr>
<tr>
<td>3</td>
<td>My organisation’s security budget is sufficient to achieve certification from reputable authorities such as ISO, NIST, PCI or others.</td>
<td>14%</td>
<td>24%</td>
<td>38%</td>
</tr>
<tr>
<td>4</td>
<td>My organisation’s security budget ensures expenditures are made efficiently (i.e., resources are not squandered).</td>
<td>19%</td>
<td>33%</td>
<td>52%</td>
</tr>
<tr>
<td>5</td>
<td>My organisation’s security budget is sufficient to curtail or minimize data breach incidents.</td>
<td>14%</td>
<td>23%</td>
<td>37%</td>
</tr>
<tr>
<td>6</td>
<td>My organisation’s security budget is sufficient to ensure policies are strictly enforced throughout the enterprise.</td>
<td>12%</td>
<td>21%</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>Average</td>
<td>14%</td>
<td>25%</td>
<td>40%</td>
</tr>
</tbody>
</table>
Figure 6 reports the combined average response to the six budget questions shown in Table 2 against average SES results. The line graph compares all four quartile results. It clearly shows that respondents’ perceptions about the adequacy of the security budget and SES results are systematically related. That is, respondents who perceive their budget for security as adequate enjoy a higher SES result than those who do not.

Security technology, controls and governance

The Security Effectiveness Framework consists of six security effectiveness metrics that are output variables used to assess organisations (see Figure 1). These are uptime, compliance, threat containment, cost management, breach prevention and policy enforcement. In this framework, a high value for each metric indicates that the organisation is efficient in the use of these resources.

Respondents were asked to rate enabling security technologies, control activities and governance practices deployed with their organisations. A five-point scale was used to rate a list of proven security technology in terms of their impact on each one of the six effectiveness metrics, from having no impact to having a very significant impact on effectiveness. The same procedure was used for control activities. Figure 7 presents the overall average results for enabling technologies, control activities and governance practices.

The number within each bar reflects the aggregate performance rating for the effectiveness metrics. The ratings range from 1 as a minimum value to 5 as a maximum value. The highest ratings were achieved for policy enforcement, compliance and threat containment. This suggests that respondents attach a lower level of importance to cost management and uptime. In addition, governance is viewed as more important than enabling technologies for policy enforcement and compliance metrics. In contrast, enabling technologies are viewed as most important for threat containment and data breach prevention.

Respondents were asked to rank six security effectiveness metrics from 6 = most important to 1 = least important. Consistent with Figure 7, policy enforcement, compliance and threat containment are viewed as the most important security measures. Cost management and uptime are viewed as less important measures for effectiveness (Figure 8).

Figure 6: Quartile comparison of respondents’ perceptions about the adequacy of the security budget and security effectiveness

Figure 7: Security metrics according to technology, controls and governance

Figure 8: Average rank of six security effectiveness metrics
Study methods

Ponemon Institute has independently completed a study that focused on operational effectiveness in the information security environment for a sample of 101 UK and European companies. Participants in this study are all highly-experienced information security leaders, including those holding the CISO title. The purpose of this research was to develop and empirically validate the Security Effectiveness Framework in terms of key variables and output metrics defined in Figure 1.

As Pie Chart 1 shows, respondents from 14 different industry sectors are represented in this study. The largest segments include industrial (18 percent), financial services (15 percent) and public sector (14 percent).

Approximately 80 percent of respondents are located in the United Kingdom. About twelve percent are located in Germany, four percent located in France and three percent located in the Netherlands.

Caveats

The study utilised a diagnostic interview method that has been successfully deployed in earlier research. However, there are inherent limitations to this type of research that need to be carefully considered before drawing conclusions from these findings.

Non-statistical sample:
The purpose of this study is descriptive inquiry rather than normative inference. This research draws upon a representative, but non-statistical sample of highly-experienced IT and IT security practitioners.

Non-response:
The current findings are based on a small representative sample of companies. An initial invitation was sent to targeted individuals in more than 500 organisations. One hundred and one individuals agreed to participate. Non-response bias was not tested so it is always possible companies that did not participate are substantially different on key aspects of security effectiveness.

Sampling-frame bias:
Because the sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is Ponemon Institute’s belief that the current sampling frame is biased toward companies with more mature data protection and information security programmes.

Unmeasured factors:
To keep the survey concise and focused, Ponemon Institute decided to omit other important variables from the analysis such as leading trends and organisational characteristics. The extent to which omitted variables might explain study results cannot be estimated at this time.
Part 2

The Security Effectiveness Framework Tool
As described above, the study was used to validate the measures that indicate the security effectiveness in an organisation. Following the validation process, Ponemon Institute streamlined the original survey to create the Security Effectiveness Framework Tool, which provides a snapshot of the effectiveness of an organisation’s security initiatives. The tool requires completion of questions relating to the following six major issues:

1. **Culture (organisational characteristics):** How does an organisation perceive itself in terms of trust, risk adversity, efficiency, strategic orientation and innovation?

2. **Security environment:** How does an organisation perceive its ability to prevent or curtail attacks and ensure there is sufficient security?

3. **Technologies:** What are the specific enabling technologies the organisation has decided to deploy?

4. **Control activities:** What are the specific control activities the organisation conducts? These can include business continuity planning and training of security practitioners.

5. **Governance:** What governance practices are implemented fully, partially or not at all in their organisations? These can include appointment of a high-level CISO and segregation of duties between CISO and IT operations.

6. **Budget:** Is the budget adequate to support investment in enabling technologies and skilled personnel to meet its security mission?

The report highlights areas that need improvement in order to achieve greater effectiveness. It also provides guidance on how to be more efficient in allocating resources. Specifically, it makes recommendations about what technologies the organisation should consider deploying, what control activities and governance practices should be used and if the budget is adequate to support improvements.

The results of the survey are summarised in several graphs and charts according to three points of reference: (1) best case, (2) worst case and (3) illustration. The illustration that follows is presented to show how the tool computes results based on average or normal assumptions.

As mentioned above, the tool is divided into six parts (input variables). It contains 77 separate survey items resulting in a total of 120 points. Items are scored as favourable yielding a positive result (+) or unfavourable yielding a negative result (-). Hence, the maximum score is 120 points (termed the best case) and the minimum score is -120 points (termed the worst case). A zero (0) represents the theoretical mean value.

*Pie Chart 2* (below) reports the percentage contribution for each input variable. As shown, organisational culture represents the smallest contribution (8 percent), followed by budget (13 percent). The largest contribution concerns the security environment (22 percent), followed by governance (21 percent). Both enabling technologies and controls are at 18 percent.

![Pie Chart 2: Input Variables](chart.png)
Pie Chart 3 (right) shows the proportional contribution of each one of the six security effectiveness metrics. These percentages are computed from the best and worst case (extremes). As reported, the most significant metric concerns policy enforcement (22 percent), followed by compliance (20 percent). The least significant metrics concern uptime and cost efficiency (both at 12 percent). Threat containment and breach prevention both contribute 17 percent to the total framework.

Figure 9 reports a combined view (for all six input variables) for security effectiveness metrics based on the survey. As shown, the maximum and minimum lines are symmetric, with the illustration charting between these extremes.

Figure 10 shows the study results for the illustration using a radar (spider) diagram. This chart highlights the strengths and weaknesses of the hypothetical company as measured in points for each metric. Specifically, breach prevention, threat containment, and uptime are seen as relatively stronger metrics, while compliance, cost efficiency and policy enforcement are weaker.

Figure 11 shows the results for the illustration in comparison to the best case. This chart clearly shows the hypothetical company as charting well below the best case for the six security effectiveness metrics.

Please note that the best-case scenario is not proportional in the allocation of its 120 points. The correct proportion or percentages is shown in Pie Chart 3. Accordingly, policy enforcement and compliance contribute the highest values, and uptime and cost efficiency represent the lowest values.
The following graphs report each one of the six effectiveness metrics in greater detail according to the six input variables.

**Figure 12** reports uptime. A comparison of best and worst case scenarios suggest uptime is influenced by security environment and governance variables and less by enabling technologies, controls and culture.

**Figure 13** reports compliance. Similar to **Figure 12**, security environment and governance have a more significant impact on compliance than enabling technologies or organisational culture.

**Figure 14** reports threat containment. Unlike the previous graphs, enabling technologies influence threat containment. Here, culture, governance and budget have only a nominal impact.

**Figure 15** reports cost efficiency. As shown, governance has the most significant influence and enabling technology, controls and culture have a nominal effect on cost efficiency.

**Figure 16** reports breach prevention. Similar to threat containment, this metric is significantly influenced by enabling technologies and controls, and less influenced by budget, governance and culture.

**Figure 17** reports policy enforcement. Clearly, governance and the security environment have the greatest impact on this effectiveness metric.
Figure 18 reports the aggregated view of all six effectiveness metrics. As shown, the most significant input variables concern the security environment and governance. The least significant variables concern culture and budget.

Figure 19 provides an alternative view to the above line graph. Here, the illustration is below the maximum or best case for all six inputs. The illustration comes closest to the best-case scenario for controls and culture variables. In contrast, the illustration is furthest away from the maximum value for governance, security environment and budget.

The final result as shown in Figure 20 is the security effectiveness rating (SER), which defines the company’s overall security effectiveness score based on responses to the organisation’s variables and measures of security effectiveness. The best case shows 120 points earned (maximum score based on a perfect performance shown in green). The worst case shows -120 points (minimum scores for compete failure on the tool shown in red). Please keep in mind that the maximum and minimum values are two extremes that are likely never to be experienced in actual practice. The figure right shows the SER score for the hypothetical organisation.
Concluding comments

The results of this study validate the importance of six security effectiveness metrics. While all six metrics for security effectiveness correspond to the Security Effectiveness Score (SES) as well as certain organisational characteristics and budget, it is clear that policy enforcement, compliance and threat containment are more salient than other metrics.

From these results, Ponemon Institute created a measurement tool that provides practical insights for IT and IT security practitioners as they strive to determine whether their organisations are achieving the highest possible effectiveness for a given level of resources.

The appendix (attached) provides a measurement tool built directly from the empirical results collected in this study. Ponemon Institute envisions that individuals will complete questions relating to:

- Adequacy of the budget.
- Specific technologies deployed.
- Specific control activities conducted.
- Specific security governance practices.
- Organisational culture.

The measurement tool captures information inputs from interviews with the assistance of trained representatives. Once data is entered into the system, the tool generates an analysis according to six effectiveness metrics with comparison to average study results. In addition to six individual metrics, the tool generates one overall security effectiveness rating.
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

As a member of the Council of American Survey Research Organisations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.
Dear respondent,

We want to learn about your organisation’s present capability to achieve an operationally effective security environment.

We appreciate your thorough responses to all benchmark survey questions. Please be assured that we will not collect any personally identifiable information. Your identity will remain completely confidential. Please contact Ponemon Institute at research@ponemon.org or call us at 1.800.887.3118 if you have any questions about this research.

Thank you in advance for your participation.

L.A. Ponemon
Dr. Larry Ponemon
Chairman & founder

Definitions:

Security posture: describes your organisation’s ability to prevent, detect and resolve internal and external threats against assets, information resources and IT infrastructure.

Security environment: the company’s overall approach to creating an effective security ecosystem.

Enabling technologies: describes specific security solutions, systems and tools used to mitigate or curtail security threats, vulnerabilities and risks.

Control activities: describes specific control procedures deployed to mitigate or curtail security threats, vulnerabilities and risks.

Governance: describes the company’s oversight structure that establishes accountability over security and data protection activities.

Uptime: the company’s ability to withstand attacks that cause systemic failure and business interruption.

Threat containment: the company’s ability to prevent or quickly detect external security threats such as cybercrime, social engineering or malicious outsiders.

Cost efficiency: the ability to manage investments in information security and data protection in a competent (non-wasteful) manner.

Breach prevention: the ability to prevent or quickly detect internal security threats such as the negligent or incompetent insider.

Policy enforcement: the ability to monitor and strictly enforce compliance with internal policies, procedures and other security requirements.
### Part 1: Organisational culture

Rate your organisation in terms of five characteristics.

<table>
<thead>
<tr>
<th></th>
<th>Agree</th>
<th>Unsure</th>
<th>Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 My organisation is a trusted enterprise.</td>
<td>2.00</td>
<td>0.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>2 My organisation tends to be risk averse.</td>
<td>2.00</td>
<td>0.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>3 My organisation strives to be efficient.</td>
<td>2.00</td>
<td>0.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>4 My organisation is strategically oriented.</td>
<td>2.00</td>
<td>0.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>5 My organisation strives to be innovative.</td>
<td>2.00</td>
<td>0.00</td>
<td>-2.00</td>
</tr>
<tr>
<td><strong>Total score</strong></td>
<td>10.00</td>
<td>0.00</td>
<td>-10.00</td>
</tr>
</tbody>
</table>

### Part 2: Security environment

Please rate your level of confidence about each statement concerning the information security environment in your organisation today.

<table>
<thead>
<tr>
<th></th>
<th>Confident</th>
<th>Not confident</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Prevent or curtail major data breaches involving sensitive or confidential information.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>2 Secure sensitive or confidential data at rest and in motion.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>3 Secure endpoints to the network.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>4 Identify and authenticate users before granting them access to sensitive or confidential information.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>5 Prevent or curtail cyber attacks.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>6 Limit physical access to data and storage devices.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>7 Ensure minimal downtime to systems resulting from security problems.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>8 Comply with legal requirements and policies.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>9 Prevent or quickly detect viruses and malware infection.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>10 Perform security updates and patches in a timely manner.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>11 Ensure sufficient security over application development activities.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>12 Enforce security and data protection policies.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td>13 Ensure third parties have adequate security practices before sharing sensitive information or critical applications.</td>
<td>2.00</td>
<td>-2.00</td>
</tr>
<tr>
<td><strong>Total score</strong></td>
<td>26.00</td>
<td>-26.00</td>
</tr>
</tbody>
</table>
### Part 3:

Please state whether each enabling security technology is implemented fully, partially or not at all in your organisation today.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Fully deployed</th>
<th>Partially deployed</th>
<th>Not deployed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Access governance systems.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>2 Anti-virus &amp; anti-malware.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>3 Code review tools.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>4 Security intelligence &amp; event management (SIEM).</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>5 Data loss prevention (DLP).</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>6 Database scanning and monitoring.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>7 Encryption for data at rest.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>8 Encryption for data in motion.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>9 Encryption for laptops and wireless devices.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>10 Endpoint security solutions.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>11 Firewalls.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>12 ID &amp; credentialing systems.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>13 Intrusion detection systems.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>14 Intrusion prevention systems.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>15 Log management.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>16 Network intelligence systems.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>17 Patch management systems.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>18 Perimeter or location surveillance.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>19 Privileged user management.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>20 End-user management &amp; provisioning.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>21 Virtual private network (VPN).</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>22 Web application firewalls (WAF).</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td><strong>Total score</strong></td>
<td><strong>22.00</strong></td>
<td><strong>0.00</strong></td>
<td><strong>-22.00</strong></td>
</tr>
</tbody>
</table>
Part 4:

<table>
<thead>
<tr>
<th>Please state whether each control activity is implemented fully, partially or not at all in your organisation today.</th>
<th>Fully deployed</th>
<th>Partially deployed</th>
<th>Not deployed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Business continuity planning.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>2 Training of end users.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>3 Frequent IT audits.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>4 Training of security practitioners.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>5 Redress &amp; enforcement.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>6 Background checks of privileged users.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>7 Secure disposal of paper documents.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>8 Upstream communications.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>9 Safe disposal of electronic data-bearing devices.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>10 Control assessment.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>11 CERT connection.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>12 Vetting &amp; monitoring of third parties.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>13 Annual external audit.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>14 Training of data handlers.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>15 Reference to benchmarks or standards.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>16 Record retention &amp; archive management.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>17 Certification of security staff.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>18 Monitoring regulatory changes.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>19 Quality assurance.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>20 Helpdesk activities.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>21 Policies &amp; procedures.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>22 Surveillance of data center and related facilities.</td>
<td>1.00</td>
<td>0.00</td>
<td>-1.00</td>
</tr>
<tr>
<td>Total score</td>
<td>22.00</td>
<td>0.00</td>
<td>-22.00</td>
</tr>
</tbody>
</table>
Part 5:
Please state whether each governance feature is implemented fully, partially or not at all in your organisation today.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Fully deployed</th>
<th>Partially deployed</th>
<th>Not deployed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Appointment of a high-level CISO.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>2 Board or audit committee oversight.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>3 Direct budgetary authority.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>4 Convergence between physical &amp; logical security.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>5 Cross-functional steering committee.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>6 Metrics or measures used to define success.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>7 Security department or function is officially sanctioned (charter).</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>8 Participation in benchmark program (with reference to peer group).</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>9 Segregation of duties between CISO and IT operations.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td>10 Upstream reporting channel to the CEO.</td>
<td>2.50</td>
<td>0.00</td>
<td>-2.50</td>
</tr>
<tr>
<td><strong>Total score</strong></td>
<td><strong>25.00</strong></td>
<td><strong>0.00</strong></td>
<td><strong>-25.00</strong></td>
</tr>
</tbody>
</table>

Part 6:
Please state Yes or No to each one of the following questions concerning your organisation’s security budget today.

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 My organisation’s security budget is sufficient to accomplish its mission and objectives.</td>
<td>3.00</td>
<td>-3.00</td>
</tr>
<tr>
<td>2 My organisation’s security budget is sufficient to ensure our IT systems are not disrupted or brought down by attackers.</td>
<td>3.00</td>
<td>-3.00</td>
</tr>
<tr>
<td>3 My organisation’s security budget is sufficient to achieve certification from reputable authorities such as ISO, NIST, PCI or others.</td>
<td>3.00</td>
<td>-3.00</td>
</tr>
<tr>
<td>4 My organisation’s security budget is sufficient to curtail or minimize data breach incidents.</td>
<td>3.00</td>
<td>-3.00</td>
</tr>
<tr>
<td>5 My organisation’s security budget is sufficient to ensure policies are strictly enforced throughout the enterprise.</td>
<td>3.00</td>
<td>-3.00</td>
</tr>
<tr>
<td><strong>Total score</strong></td>
<td><strong>15.00</strong></td>
<td><strong>-15.00</strong></td>
</tr>
</tbody>
</table>
Part 7:

Please complete the following questions about your background and other company-related information.

**Your current title is:**

**D1. What organisational level best describes your current position?**
- [ ] Senior Executive
- [ ] Vice President
- [ ] Director
- [ ] Manager
- [ ] Supervisor
- [ ] Technician
- [ ] Staff
- [ ] Contractor
- [ ] Other

**D2. Is this a full time position?**
- [ ] Yes
- [ ] No

**D3. Check the Primary Person you or your IT security leader reports to within the organisation.**
- [ ] CEO/Executive Committee
- [ ] Chief Financial Officer
- [ ] General Counsel
- [ ] Chief Information Officer
- [ ] Compliance Officer
- [ ] Human Resources VP
- [ ] Chief Security Officer
- [ ] Chief Risk Officer
- [ ] Other

**D4. Total years of relevant experience**
- [ ] Total years of IT or security experience
- [ ] Total years in current position years

**D5. Gender:**
- [ ] Female
- [ ] Male

**D6. What industry best describes your organisation’s industry focus?**
- [ ] Airlines
- [ ] Automotive
- [ ] Brokerage & Investments
- [ ] Communications
- [ ] Chemicals
- [ ] Credit Cards
- [ ] Defense
- [ ] Education
- [ ] Energy
- [ ] Entertainment and Media
- [ ] Federal Government
- [ ] Food Service
- [ ] Healthcare
- [ ] Hospitality
- [ ] Manufacturing
- [ ] Insurance
- [ ] Internet & ISPs
- [ ] State or Local Government
- [ ] Pharmaceuticals
- [ ] Professional Services
- [ ] Research
- [ ] Retailing
- [ ] Retail Banking
- [ ] Services
- [ ] Technology & Software
- [ ] Transportation

**D7. Where are your employees located? (check all that apply):**
- [ ] United Kingdom
- [ ] Europe
- [ ] North America
- [ ] Middle east
- [ ] Asia-Pacific
- [ ] Latin America

**D8. What is the worldwide headcount of your organisation?**
- [ ] Less than 500 people
- [ ] 500 to 1,000 people
- [ ] 1,001 to 5,000 people
- [ ] 5,001 to 25,000 people
- [ ] 25,001 to 75,000 people
- [ ] More than 75,000 people
Contact Information:

For more information please contact us at:

Or visit:
www.hp.com/info/security