The Cyber Security Leap: From Laggard to Leader

High performance. Delivered.

accenture

Strategy | Consulting | Digital | Technology | Operations

Contents

Introduction

If your company is like most, security has risen to the top of the agenda amongst C-suite executives and boards of directors. Rapidly evolving security threats pose an ongoing, central challenge, as companies and governments face an increasingly sophisticated threat environment. Large global organizations with industry presence and value may be of special interest for adversaries, whether they be individuals, organized crime or nation states. Forrester predicts that at least 60 percent of enterprises will discover a breach in 2015, but says the actual number of breached entities will be much higher–80 percent or more.[1]

How can organizations become more effective in meeting increasing security challenges? How can organizations more quickly detect security threats, malicious attacks and data breaches? For those looking to improve their overall security posture and establish programs that can help improve their ability to detect and respond to various security threats, the time to evaluate strategy and capabilities is now.

Accenture, in collaboration with the Ponemon Institute LLC, conducted a study to identify the success factors of companies that demonstrated at least 25 percent improvement in Security Effectiveness Scoring over a period of two years, and an average gain of 53 percent, the Leapfrogs. The study encompassed 237 organizations, divided into those who had significantly increased their security performance and those who remained static. The research identified important differences in how the two groups addressed security strategy, innovation, technology and governance. For example, characteristics of effective security strategies include alignment with business objectives and accountability throughout the organization. Leapfrog organizations recognize the need for innovation to strengthen their security position and keep pace with evolving needs. The use of enabling and advanced technologies helps the Leapfrog companies take a proactive stance to protect their networks and data. Governance measures such as metrics, benchmarking, risk management procedures and ongoing communications with the C-suite and board of directors reflect the importance that the Leapfrog organizations place on their security policies and programs.

Ready to leapfrog?

Security is a top business priority for Leapfrog companies, and it's aligned with the organization's strategic goals. This is evidenced by a focus on innovation to achieve a strong security posture, open communication with the CEO and corporate boards on security incidents, and deployment of enterprise risk management procedures.

Leapfrog companies embrace new and disruptive security technologies as part of their strategy, and are proactive in responding to major changes in the threat landscape. CISO has the authority to define and manage the company's security strategy. Finally, budget and spending levels for security and security innovation steadily increased for these companies over the past two years.

For Static companies, however, security operates under a veil of stealth, secrecy and underfunding. Security efforts focus on prevention and prioritizing external threats. Security programs are driven by compliance with regulations and policies, and security is viewed as a trade-off with employee productivity. CISOs of Static companies describe their budgets as inadequate for meeting the company's security mission.

Key study findings

In examining the characteristics of Leapfrog and Static companies, key themes emerged:

THEME 1

Innovation and strategy separate Leapfrog from Static companies

THEME 2

Leapfrog organizations respond to changes in the threat landscape

THEME 3

CISO is a strategic role

THEME 4

Importance of controls and governance practices

THEME 5

Security technologies that support Leapfrog companies

THEME 6

Leapfrog companies invest in security

THEME 1
Innovation and strategy: separating the leapfrogs from the laggards

Security innovation is valued by Leapfrog companies

Leapfrog companies have made significant increases to their level of security innovation, seeking out new approaches to emerging problems. In trying to address what's to come, Leapfrog organizations work to develop the next generation of solutions, collaborating with groups such as universities, research and development organizations, venture capitalists or start-ups to shape their technology landscape. In contrast to Static companies, Leapfrog companies are more likely to place significant importance on security innovation in order to achieve a strong security posture (Figure 1).

Leapfrog companies are more likely to have an officially sanctioned security strategy, and this strategy is more likely to be the main driver to their organization's security program. There are multiple security strategy characteristics where Leapfrog companies excel over Static companies (Figure 2).

A sound security strategy is clearly a priority for Leapfrog organizations, and the results show that many (68 percent) have significantly changed their approach to security management in recent years. Changes could include creating a new CISO role, allocating dedicated security budget or significantly expanding the security team. Leapfrog companies are more likely to consider information security a business priority and align their security objectives with business objectives. They view security as an enabler to achieving business objectives, and are able to adapt if security hinders their objectives in exceptional situations ("Business needs sometimes trump security requirements").

Figure 1. Perceptions about the state of security innovation
Items scored using 10-point scales

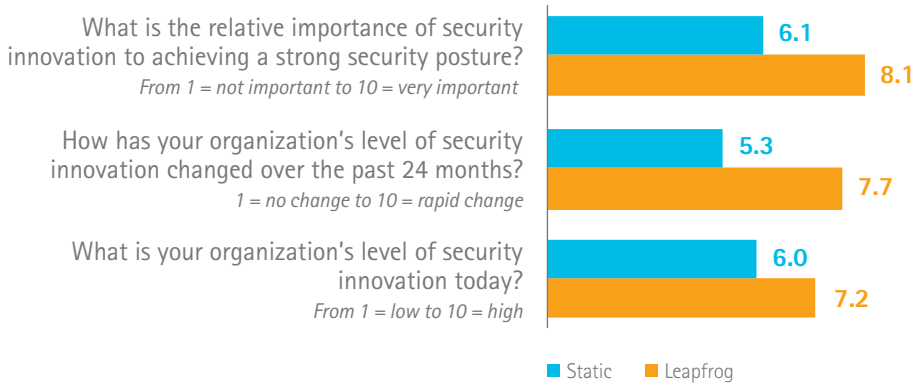
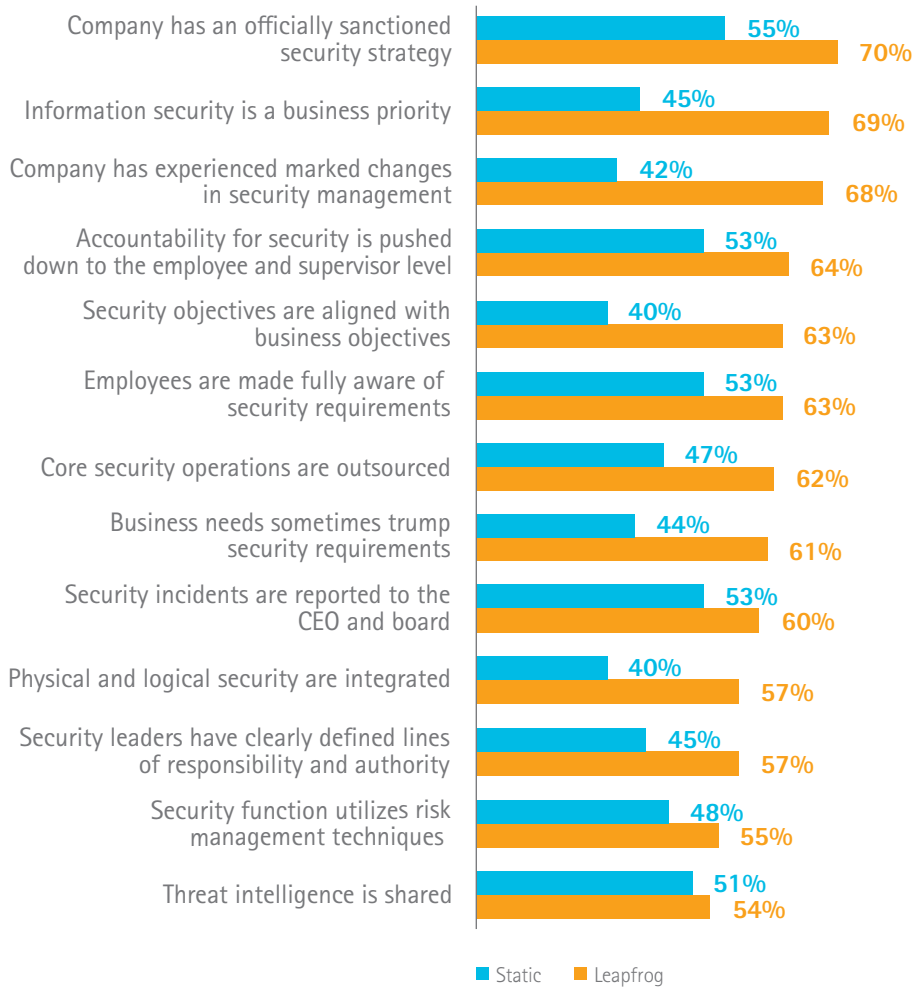


Figure 2. Strategy characteristics where Leapfrog companies excel
Percent "yes" response



Security incidents that happen within Leapfrog companies are more likely to be reported to the CEO and board of directors. The Leapfrog companies use risk management techniques to determine their security strategy and integrate physical and logical security systems. Responsibilities and authority pertaining to security are clearly defined. Employees are not only made aware of security requirements, but held accountable for following security processes.

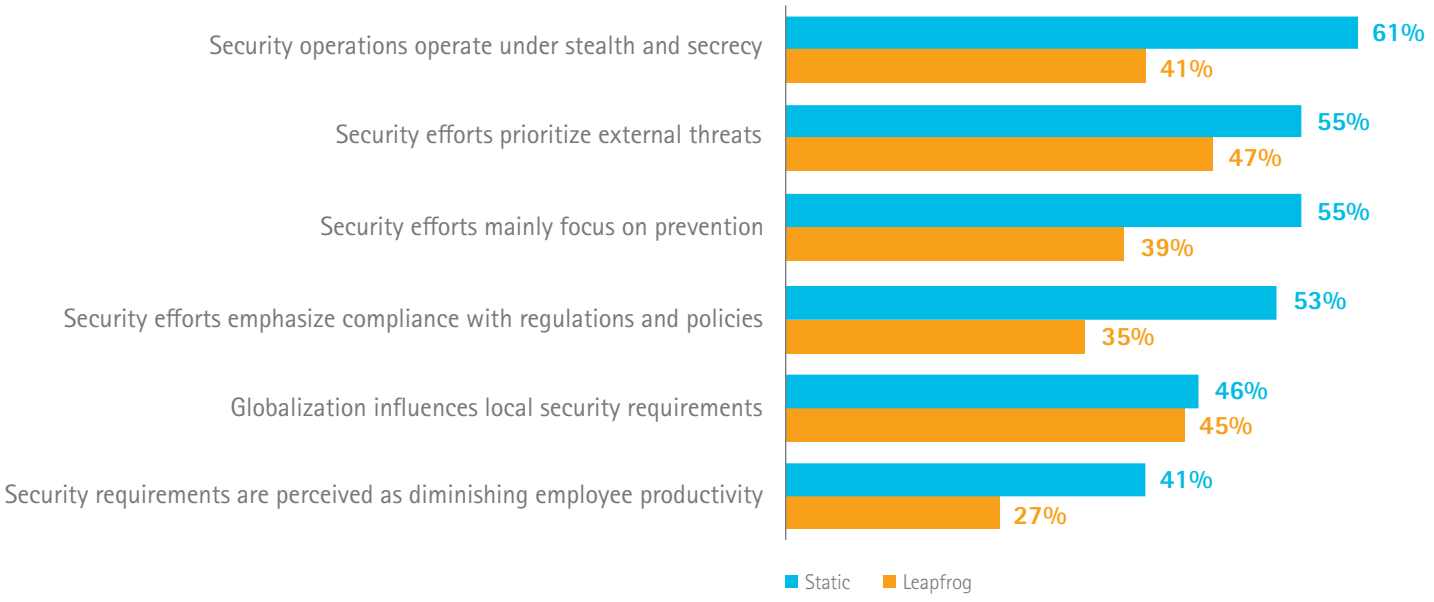
Many Leapfrog companies outsource core security operations, which can significantly increase their security effectiveness without requiring extensive investments in technology or expert resources. Outsourcing can introduce risk, so it's critical to evaluate what can be outsourced and then select the right managed services company–with this approach, Leapfrog organizations have been able to mature their security functions rapidly.

While Leapfrog and Static organizations rank almost equally in sharing threat intelligence, the other characteristics listed in Figure 2 demonstrate that simply exchanging information is not enough for effective security. Security intelligence is important. However, organizations need to be able to ingest it in order to respond appropriately.

In contrast to the Leapfrog characteristics, Static companies are more likely to operate their security policies under stealth and secrecy, and view security as diminishing to employee productivity. There are key security program characteristics that dominate Static organizations (Figure 3).

Static organizations believe that regulations, rather than strategy, drive the organization's security requirements. Security efforts focus on external threats, and are more likely to emphasize prevention rather than detection or containment. These types of characteristics do not support companies making significant improvements in the effectiveness of their security posture.

Figure 3. Characteristics of Static organizations
Percent "yes" response



THEME 2
Leapfrog organizations respond to changes in the threat landscape

Leapfrog organizations are proactive in addressing major changes to the threat landscape

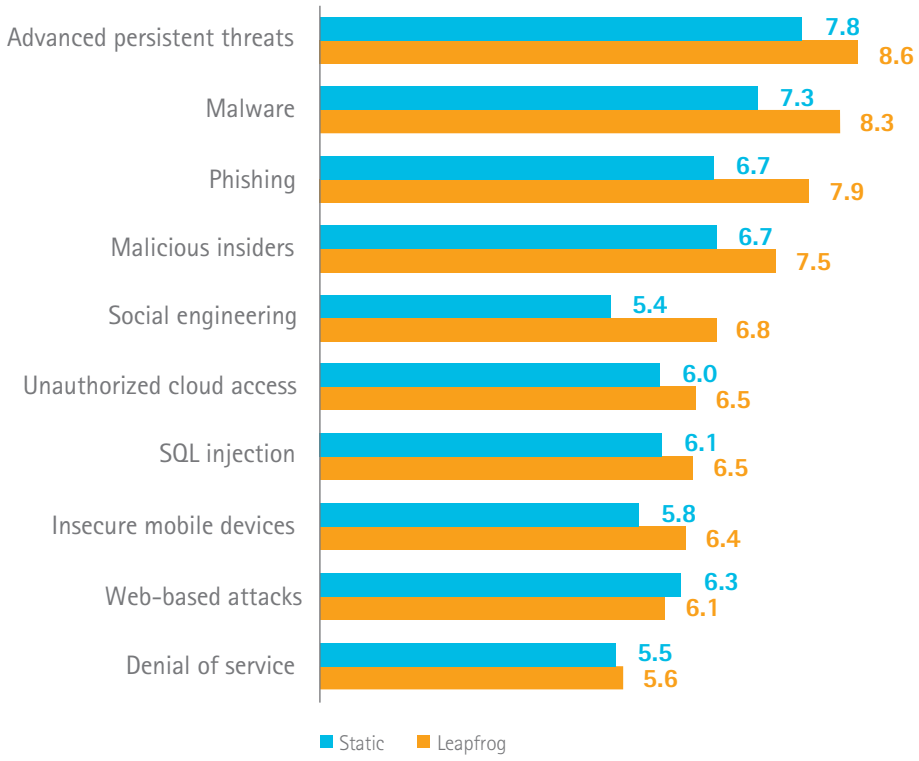
They recognize that persistent attacks should change the company's approach to IT security and adapt their security posture in response to threats. Different security threats continue to emerge—the research evaluated the level of impact those threats had on the organizations' security ecosystem and how the organizations responded (Figure 4).

The biggest changes to security strategy in Leapfrog organizations were made in response to advanced persistent threats (APTs) and malware. In comparison to Static companies, Leapfrog companies also made more significant changes in response to phishing, malicious insiders and social engineering. Examples of the changes implemented by Leapfrog companies include specialized training and awareness activities to help employees recognize phishing emails and the implementation of sophisticated monitoring tools to identify suspicious employee behaviors.

Static companies appear to be less proactive in changing their security strategy when new and emerging developments occur.

Figure 4. Impact of emerging threats on the security ecosystem

Items scored using a 10-point scale from 1 = low to 10 = high impact on security ecosystem



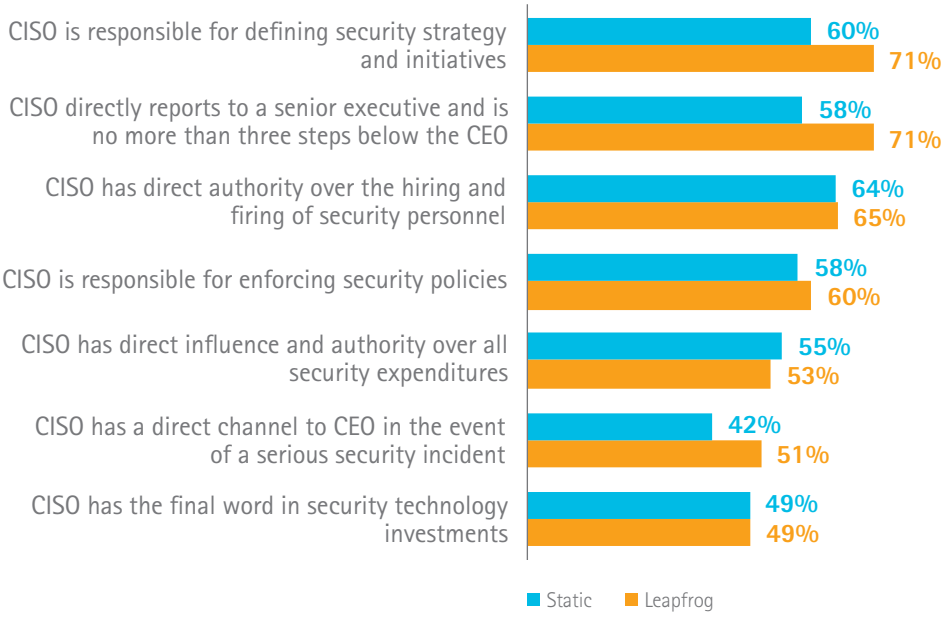
THEME 3
CISO is a strategic role

Both Leapfrog and Static organizations have a CISO; the important differences lie in how that role is viewed and executed. Across all organizations studied, the CISO has hiring/firing authority, holds responsibility for enforcing security policies and has authority over budget and investment decisions.

Within Leapfrog organizations, however, the CISO is more likely to directly report to a senior executive, set the security mission by defining strategy and initiatives, and have a direct channel to the CEO in the event of a serious security incident.

Since both Leapfrog and Static organizations have CISOs, the existence of that role within an organization is not a determining factor in security effectiveness. What matter are factors that reflect the strategic value of the CISO—including the ability to define security strategy and programs, and the relationship between the CISO, the CEO and the board of directors. In Static organizations, that relationship is filtered through several levels of operational management, muting the true picture of operational risk needed to guide the business.

Figure 5. The CISO role in Leapfrog and Static organizations



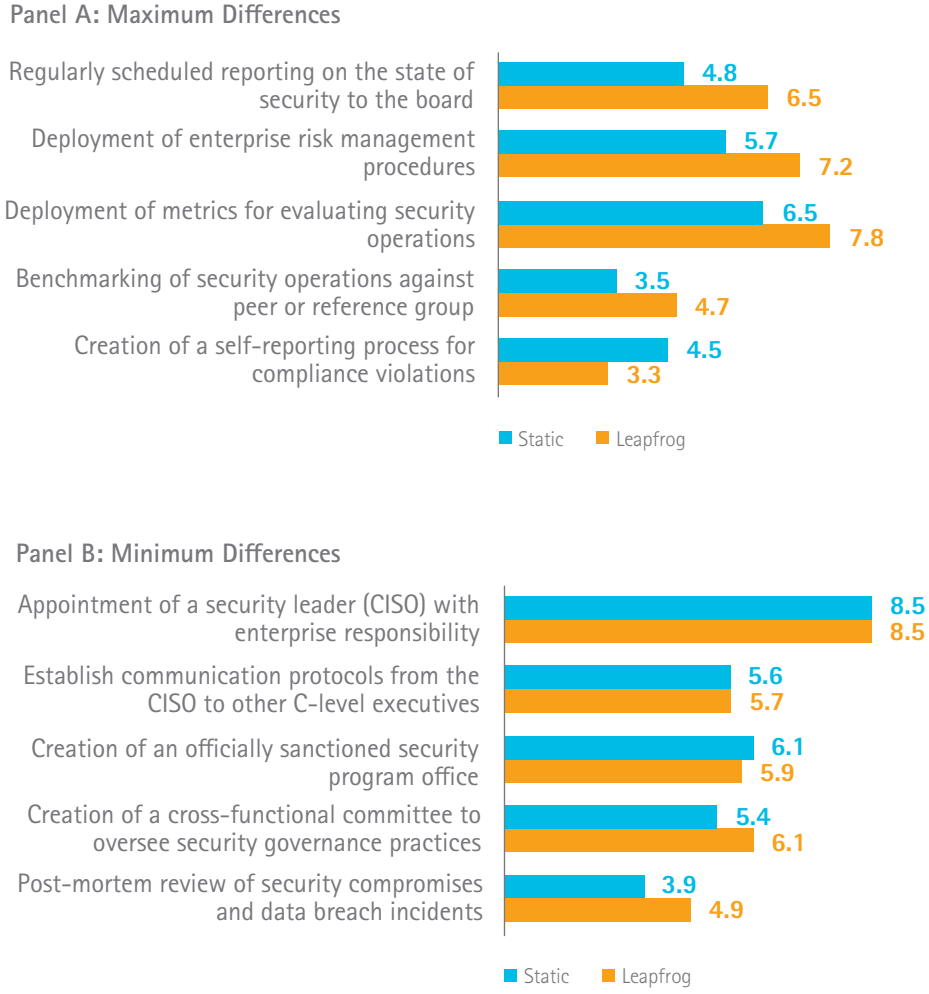
THEME 4
Importance of controls and governance practices

Leapfrog companies excel in governance

Both groups of companies identified the importance of appointing a CISO for the organization, recruiting expert IT security personnel and background checks for all privileged users as critical to achieving a strong security posture. However, the Leapfrog companies believe disaster recovery and business continuity management practices are important. Static companies, on the other hand, are more likely to cite clearly defined IT security policies and standard operating procedures (SOP) than Leapfrog companies.

The governance practices of Leapfrog and Static companies vary significantly by attribute (Figure 6). Leapfrog companies are more likely to have advanced governance practices—ranging from regular reports on the state of security to the board, to deployment of enterprise risk management procedures. They are more likely to adopt metrics for evaluating security operations, benchmarking of security operations against peers or reference groups, and conduct post-mortem reviews of security compromises and data breach incidents. Static companies are more likely to create a self-reporting process for compliance violations, which can be less effective. Strong governance and controls lead to established security policies, clearly defined responsibilities and accountability. A good security posture is achieved when decisions follow structured policies, helping the organization's risk remain at acceptable levels.

Figure 6. Governance practices of Leapfrog and Static companies
Items scored using a 10-point scale from 1 = not important to 10 = very important



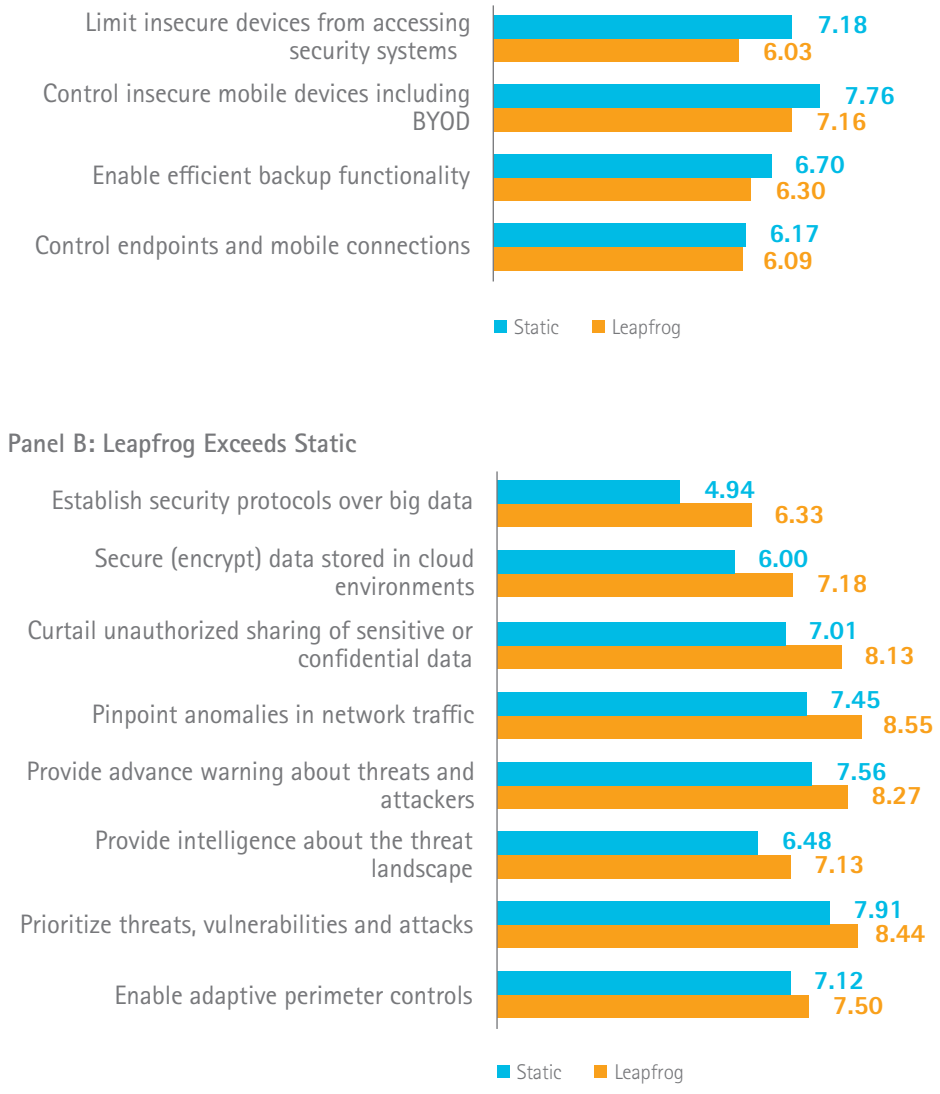
THEME 5
Security technologies that support Leapfrog companies

Certain technologies separate Leapfrog and Static companies

Leapfrog companies exceed Static companies in viewing the following features of security technologies as very important: pinpointing anomalies in network traffic; prioritizing threats, vulnerabilities and attacks; curtailing unauthorized sharing of sensitive or confidential data; and enabling adaptive perimeter controls (Figure 7). In contrast, Static companies exceed Leapfrog companies in believing the following are more important features of security technologies: controlling insecure mobile devices including BYOD, limiting access for insecure devices and enabling efficient backup functionality.

Leapfrog companies demonstrate higher engagement with new and disruptive technologies; they also focus more on securing the network and the cloud, as opposed to focusing on individual devices. Static companies tend to focus on locking things down, which can prevent business growth. Within Leapfrog companies, business strategy is used to inform security strategy.

Figure 7. Features of enabling security technologies for Leapfrog and Static companies
Items scored using a 10-point scale from 1 = not important to 10 = very important



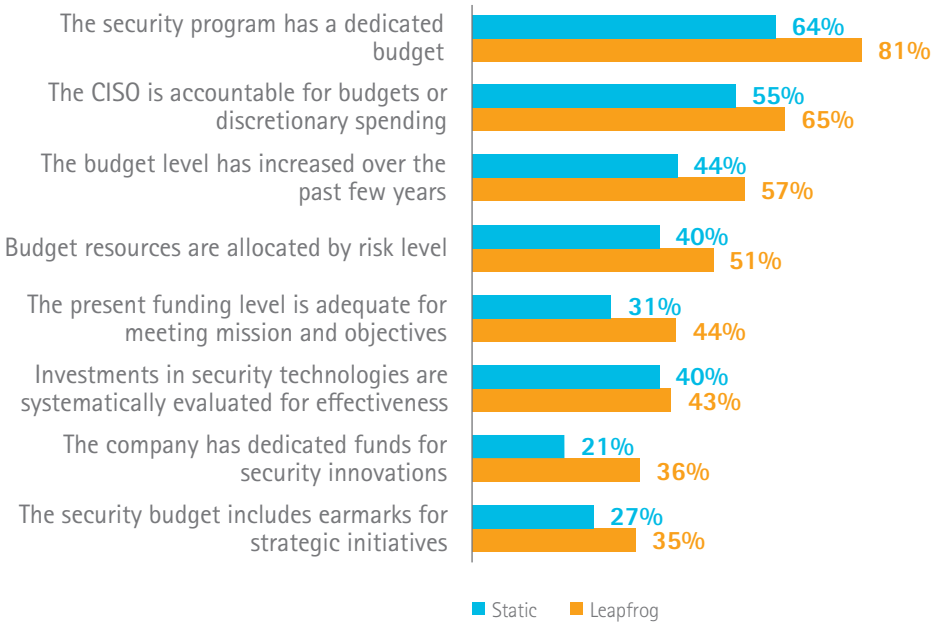
THEME 6
Leapfrog companies invest in security

Security budgets in Leapfrog companies include funding for innovations in information technologies

Leapfrog companies are more likely to have a dedicated budget for its security programs and have allocated more money toward security over the past few years (Figure 8). They also have a fund dedicated to innovations in information technologies. These companies are more positive about having enough funding to meet their mission and objectives.

In contrast to Leapfrog companies, Static companies are less likely to have a dedicated budget for their security programs, have more budget resources allocated to prevention than detection activities and are also less likely to spend on strategic initiatives.

Figure 8. Security budget considerations for Leapfrog and Static companies



Research predictions

Benchmark interviews with participating companies allowed us to compile a subjective probability estimate of a material data breach involving the loss or theft of 10,000 or more records. Leapfrog companies experienced a negative percentage change, which means the likelihood of material data breaches has decreased over time (Figure 9). In contrast, Static companies experienced a positive percentage change, indicating that the perceived likelihood of material data breaches has slightly increased over time.

Similar to the above analysis, our benchmarking process allowed us to compile a subjective probability estimate for the theft or exfiltration of high-value information. Leapfrog companies experienced a reduction in the likelihood of exfiltration of intellectual property over time (Figure 10). In contrast, Static companies experienced a positive percentage change, indicating that the perceived exfiltration risk has increased over time.

Figure 9. Net change in the probability of a significant disruption

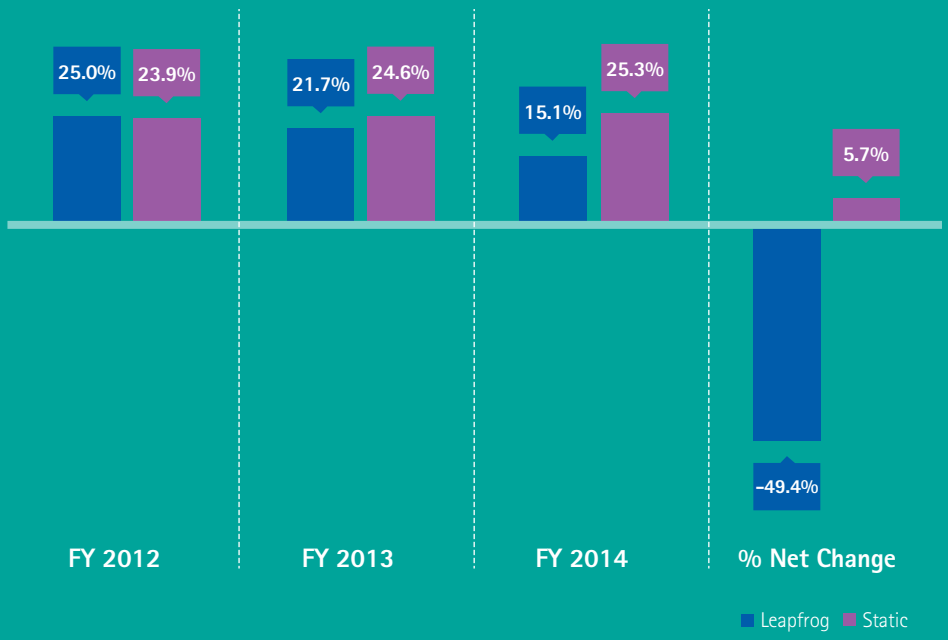
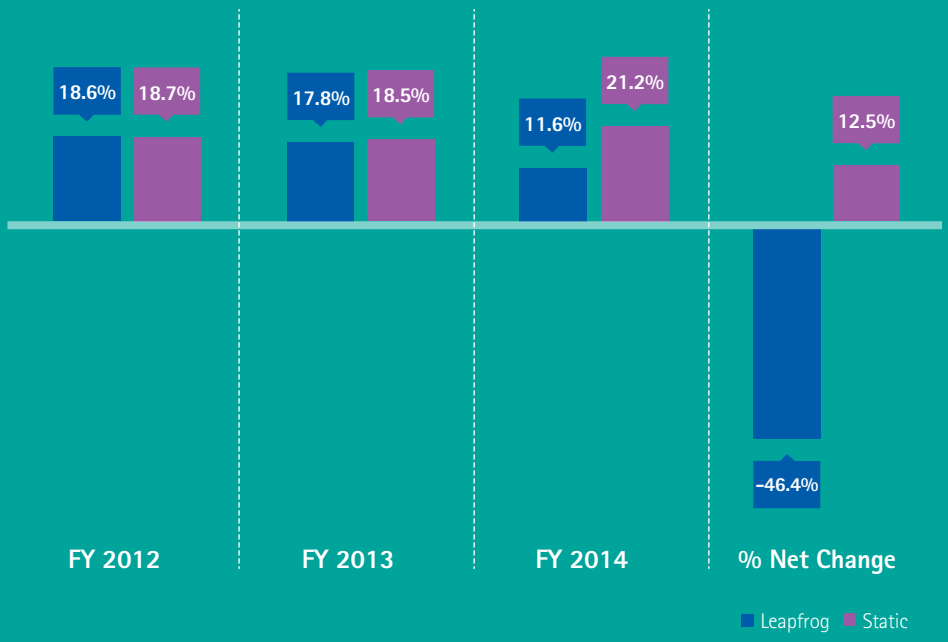
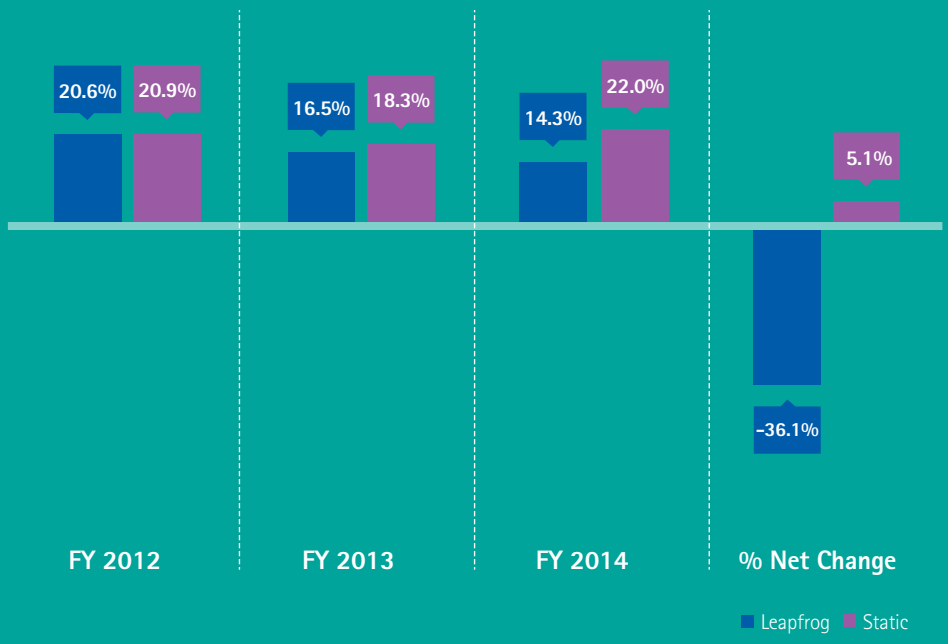


Figure 10. Net change in the probability of high-value information theft



We also compiled subjective probability estimates that Leapfrog and Static companies would experience a substantial cyber attack that could disrupt business operations or IT infrastructure (Figure 11). Here again, Leapfrog companies experienced a negative percentage change, which means the perceived likelihood of substantial disruptions has decreased over time. Static companies experienced an increase over time.

Figure 11. Net change in the probability of a material data breach



Conclusion

The scale and scope of recent breaches have made security top of mind for the C-suite and boards of directors around the globe. Cyber security posture and cyber defense capabilities are at the forefront of business resilience and brand trust. Lost reputation is the number one consequence experienced by companies, with 52 percent of companies saying loss of reputation, brand value and marketplace image were the biggest impacts of a data breach.[2] Costs relating to security breaches are also extensive. The average time to contain a cyber attack is 31 days, with an average cost of $639,462 during that period.[3]

Traditional monitoring defenses are inadequate. Organizations must use advanced techniques to identify and contextualize threats. Studying and implementing the practices exhibited by Leapfrog organizations can provide an approach to help improve security effectiveness, within a relatively short time frame.

Are you ready to more tightly align a strong security strategy with your organization's business goals? Starting with the C-suite, it's time to champion and achieve a strong security posture—effectively communicating with all employees. By holding everyone accountable for achieving security objectives, you will eliminate security silos within your organization.

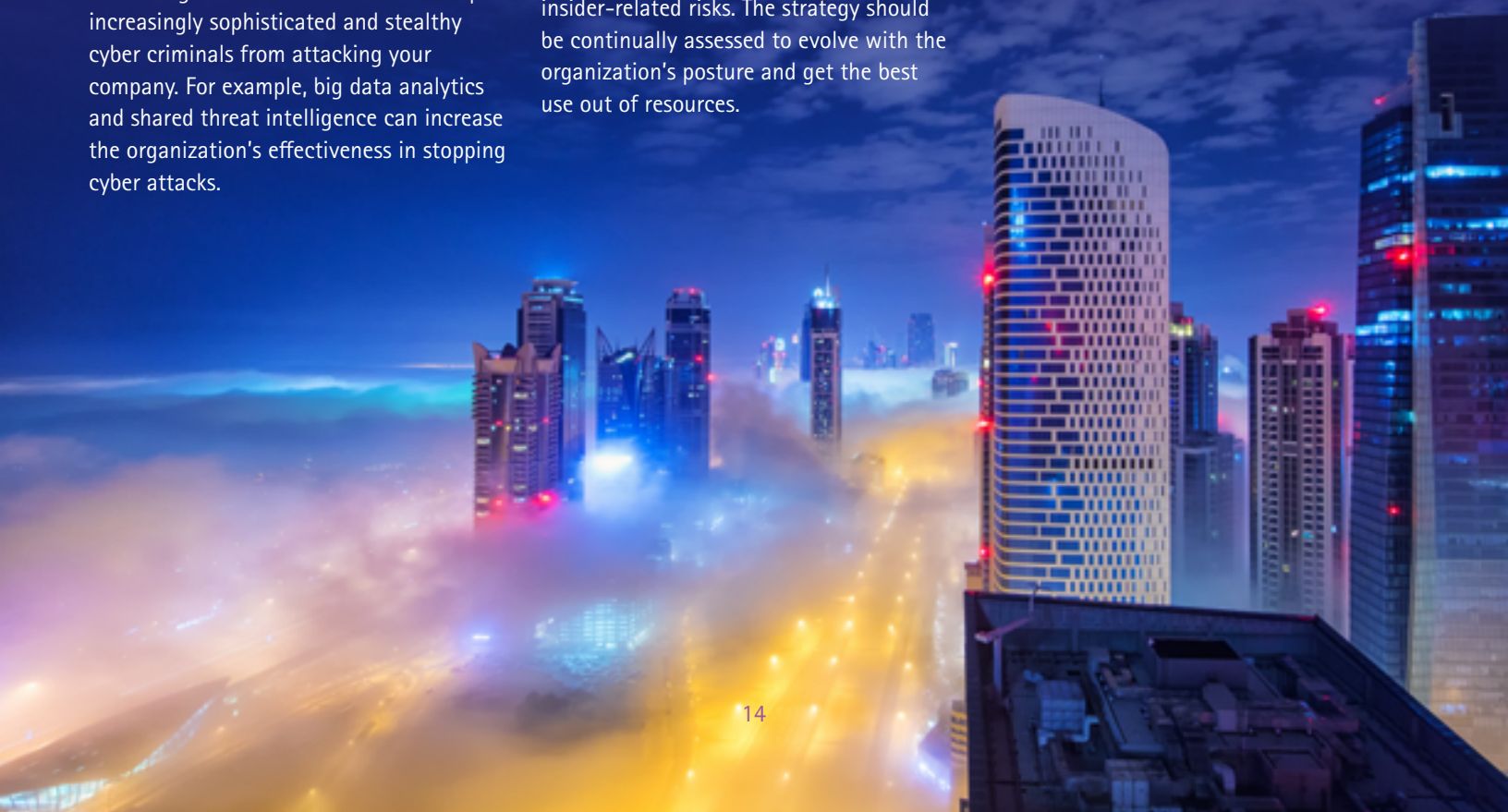
Embracing innovative solutions will keep increasingly sophisticated and stealthy cyber criminals from attacking your company. For example, big data analytics and shared threat intelligence can increase the organization's effectiveness in stopping cyber attacks.

Leverage advanced technologies and innovation to proactively develop security capabilities that enhance the user experience and productivity. Balance efforts across prevention, detection and response. Companies should actively invest in security intelligence technologies to improve threat identification and enable cyber defense, while also streamlining the IT security infrastructure to avoid redundancy and complexity.

As part of establishing better governance and controls, CISOs should foster a strong working relationship with their boards and create greater visibility into business processes. They need to educate and collaborate to successfully articulate and prioritize business risk, including insider-related risks. The strategy should be continually assessed to evolve with the organization's posture and get the best use out of resources.

In conclusion, Leapfrog companies are taking an active stance. The questions for leaders are: How well is your organization positioned to actively defend your business? What will your company do to expand and innovate—with the confidence of knowing your security investment is an enabler of strategic growth?

Hop in the driver's seat and consider the recommended measures outlined from the research. You can leapfrog your company's security position, align your business goals and proactively make your move to address the changing threat landscape to achieve high performance.



Research methodology

This research looks to identify the main factors contributing to an organization's improved security posture—or leapfrogging from a level of low to high performance in its security ecosystem.

To estimate the security posture of organizations, we used the Security Effectiveness Score (SES) as part of the survey process.[4] The SES was developed by Ponemon Institute in its annual encryption trends survey to define the security effectiveness of responding organizations. We define an organization's security effectiveness as being able to achieve the right balance between efficiency and effectiveness across a wide variety of security issues and technologies.

The SES is derived from the rating of 48 security features or practices. This method has been validated by more than 60 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). A result for a given organization greater than zero is viewed as net favorable, which means the organization's investment in people and technology is both effective in achieving its security mission and efficient. Hence, they are not squandering resources and are still being effective in achieving their security goals. A negative SES has the opposite meaning.

For this research, we evaluated hundreds of companies that were previously benchmarked so that changes in the organizations' SES scores could be measured and evaluated. Based on that analysis, we divided the sample into the following groups:

Leapfrog sample: 110 companies that experienced a 25 percent or greater increase in their SES over a two-year period. The average increase in SES for these companies was 53 percent.

Static sample: 137 companies that experienced no more than a 5 percent net change in their SES over a two-year period, with an average change of 2 percent. This sample was matched to the Leapfrog sample based on industry, size and global footprint.

In this report we describe the differences between these companies in an effort to understand how companies can advance from laggard to leader. The factors addressed in this research encompass strategy, technology and governance.

Benchmark characteristics

Leapfrog Static

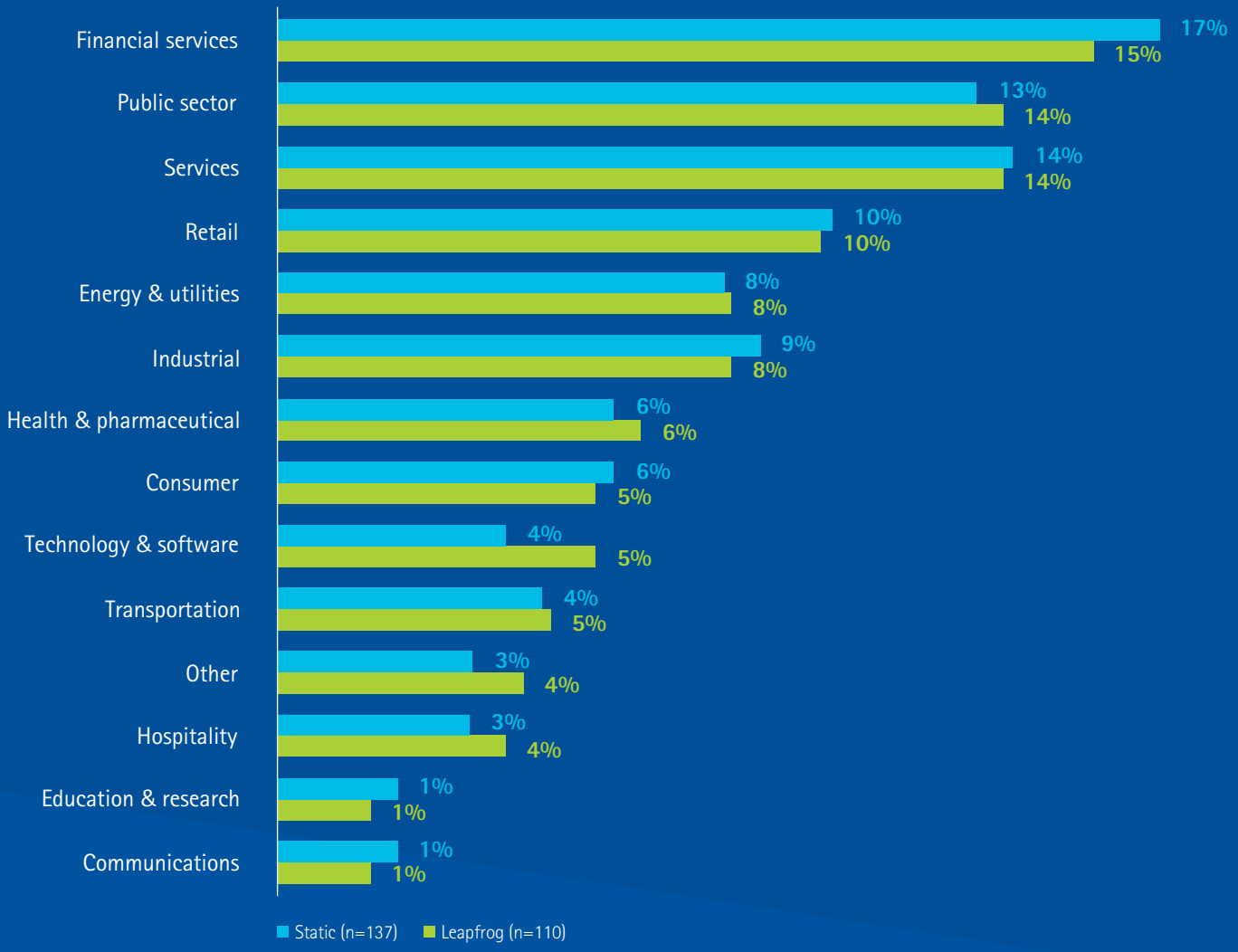
We interviewed senior-level IT and IT security practitioners from the 247 companies identified in the SES analysis to determine how these organizations were responding to security requirements and related challenges. From those interviews, common characteristics for each type of company emerged.

A total of 247 companies participated in this study. All companies were previously benchmarked and cataloged in Ponemon Institute's proprietary database consisting of 1,208 companies (at the time of this research). Our first step was to identify companies that experienced a 25 percent or greater increase in their SES over a two-year period. This resulted in 110 Leapfrog companies.

Our second step was to select a second independent sample that did not experience an increase in SES over two years. The sample was then matched to the Leapfrog sample based on industry, headcount and global footprint. This resulted in 137 Static companies.

The industry of benchmarked organizations for Leapfrog and Static was well distributed. As can be seen, financial services, public sector (government), services and retail organizations represent the four largest segments (Figure 12).

Figure 12. Distribution of the Leapfrog and Static samples by industry segment



As can be seen, the majority of companies in both Leapfrog and Static samples are larger-sized organizations with 5,000 or more full-time equivalent employees (Figure 13).

Data collection methods did not include actual tests of each company's security posture, but instead relied upon self-assessment and survey. The benchmark instrument required knowledgeable individuals within each company to rate security-related characteristics using objective questions with fixed-formatted scales.

To keep the benchmarking process to a manageable size, we carefully limited items to only those activities considered crucial to the measurement of IT or cyber security characteristics. Based upon discussions with learned experts, the final set of items included a fixed set of cost activities. Upon collection of the benchmark information, each instrument was reexamined carefully for consistency and completeness.

For purposes of complete confidentiality, the benchmark instrument did not capture any company-specific information. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

Figure 13. Distribution of the Leapfrog and Static samples by employee headcount

Validation of the SES for the Leapfrog and Static matched samples

The average SES index values were used to define and bifurcate two matched samples (Figure 14). It clearly shows the Leapfrog sample as significantly improving its SES (two-year net change at 0.286), while the Static sample shows only a nominal increase (two-year net change at 0.008).

This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations with this benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results:** Our study draws upon a representative, non-statistical sample of organizations. Statistical inferences, margins of error and confidence intervals cannot be applied to this data given that our sampling methods are not scientific.

- **Non-response:** The current findings are based on two matched samples defined by net change in SES index values over two years. This benchmarking process did not include tests for non-response. Hence, it is always possible companies that did not participate are substantially different in terms of underlying security posture.

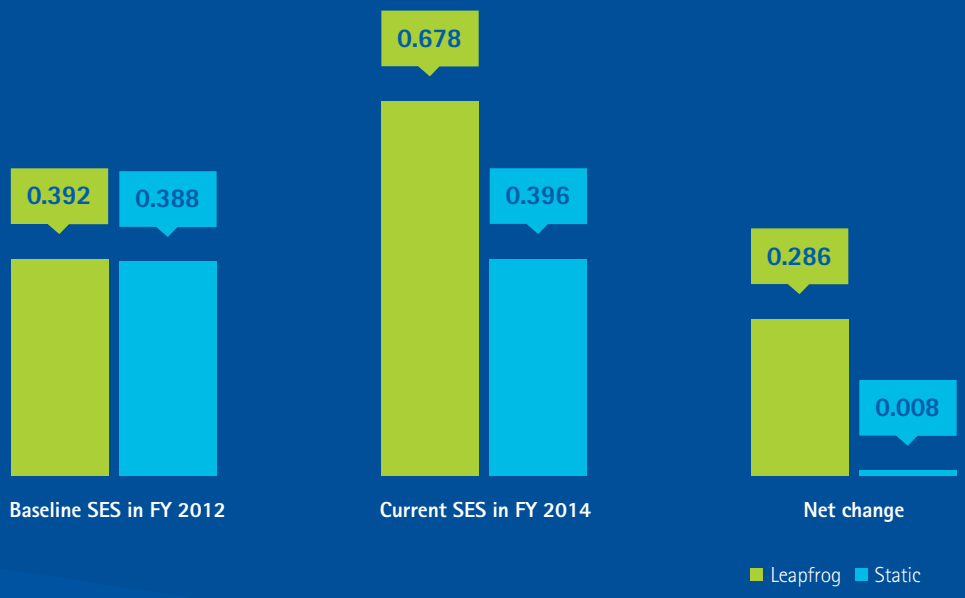
- **Sampling-frame bias:** Our sampling frame is a proprietary benchmark database created and maintained by Ponemon Institute for more than a decade. We acknowledge that the quality of empirical results is influenced by the degree to which the sampling frame is representative of the population of companies being studied. Further, it is our belief that the current sampling frame is biased toward larger-sized organizations with more mature IT security programs.

- **Company-specific information:** The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

- **Unmeasured factors:** To keep the interview script concise and focused, we decided to omit other important variables from our analyses. The extent to which omitted variables might explain benchmark results cannot be determined.

- **Extrapolated cost results:** The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate responses.

Figure 14. Net change in SES over two years for Leapfrog and Static samples
SES Index is a continuous value between -2 and +2.



For more information

Bill Phelps
Managing Director
Global Security Practice Lead
bill.phelps@accenture.com

Ryan LaSalle
Managing Director
Security Strategy Lead
ryan.m.lasalle@accenture.com

Lisa O'Connor
Managing Director
Security R&D Lead
Accenture Technology Labs
lisa.oconnor@accenture.com

Research Lead

Dr. Malek Ben Salem
Security Research and Development
Accenture Technology Labs
malek.ben.salem@accenture.com

About Ponemon Institute LLC

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 organizations.

As a member of the **Council of American Survey Research Organizations (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. For more information, visit www.ponemon.org.

About Accenture Technology Labs

Accenture Technology Labs, the dedicated technology research and development (R&D) organization within Accenture, has been turning technology innovation into business results for more than 20 years. Our R&D team explores new and emerging technologies to create a vision of how technology will shape the future and shape the next wave of cutting-edge business solutions.

Working closely with Accenture's global network of specialists, Accenture Technology Labs helps clients innovate to achieve high performance. The labs are located in Silicon Valley, California; Sophia Antipolis, France; Arlington, Virginia; Beijing, China and Bangalore, India. For more information, please visit www.accenture.com/technologylabs.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 336,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

[1]Forrester Research, Inc., "Predictions 2015: Security Budgets will Increase, as will Breach Costs, Fines and Lawsuits," November 12, 2014. (https://www.forrester.com/Predictions+2015+Security+Budgets+Will+Increase+As+Will+Breach+Costs+Fines+And+Lawsuits/quickscan/-/E-res117864)

[2]"2014: A Year of Data Breaches" (Sponsored by Identity Finder), Ponemon Institute: January 2015

[3]2014 Global Report on the Cost of Cyber Crime, Ponemon Institute: October 2014

[4]The Security Effectiveness Score is a proprietary tool developed by Ponemon Institute. For more information, please contact Ponemon Institute at research@ponemon.org.