CISO Survey and Report 2013

Version 1.0.1 (January 2014)

Project Lead and Main Author

Tobias Gondrom

Co-authors, Contributors and Reviewers

Marco Morana, Stephanie Tan and Colin Watson

Further Acknowledgement

And many more helping hands from OWASP chapters around the world were involved, providing input, designing questions, translating and sending out the survey questions around the globe.

Balint Szabo, Eoin Keary, Israel Bryski, Ivy Zhang, Jasmine Beg, Kate Hartman, Lorna Alamri, Mauro Flores, Rex Booth and Timur kHrotko

And last but not least, a special thank you to the many CISOs from around the world who took the time to fill out the Survey and offered their input and advise.

Thank you all! We couldn't have done it without you!

Chief Information Security Officers (CISOs) are responsible for application security from governance, compliance and risk perspectives. The yearly OWASP CISOs Survey and Report 2013 seeks to provide tactical and strategic intelligence for senior managers to support their application security decisions and programs.

Foreword

There is no question that application security has become a serious concern in almost every organization and industry. And more and more, application security is taking center stage in the struggle to keep information systems safe and the stored data protected. OWASP created this survey to provide senior managers with an opportunity to compare their organizations with others on important application security issues and gain insights for making key decisions. The questionnaire consisted of 26 in-depth questions concerning security investments and challenges, threats and risks, tools and technology, and governance and control within the various surveyed organizations. This research report with the results is publicly available on the owasp.org website. OWASP will be further refining our CISO survey in 2014 and increasing the collected data sets. In case you are interested in participating or providing feedback and insights, please provide your contact information, and we will contact you shortly. We take confidentiality very seriously and make sure that all personal identifiable individual and company information is NOT disclosed nor published in the survey report.

This survey report is in sync with the recently released the OWASP Application Security Guide for CISOs. These two projects are designed to harmoniously complement each other, the CISO report providing the tactical intelligence and the CISO guide offering the guidance on how CISOs can act on this intelligence to achieve the optimal information security programs for their organizations.

With best regards,

On behalf of the Project Team,

Tobias Gondrom

OWASP Global Board Member

Contents

Executive Summary

People often ask us which results of the CISO survey report, we as a fellow CISOs would find particularly interesting and useful. There are many good insights and learning points from this report. And the benefits of it will depend a lot on your own organization's maturity and security status. For some the overall strategic picture of application security risks and threats is useful to set their security priorities and strategies for next year, for others the list of best practices and recommendations from other CISO peers is particularly useful and others find most valuable to understand which best practices and tools work best for their peers.

Some of the findings we found interesting to highlight were:

1. Application security risks are clearly on the rise, in absolute numbers and also relative to infrastructure security risks.
2. Risks from external threats are clearly increasing for organizations.
3. Security awareness and training is the biggest challenge and most important priority for CISOs going forward into 2014 (more critical than tools, testing or budget).
4. As we hear from a number of CISOs about difficulties acquiring an adequate budget, it appears that having a 2-year security strategy improves your chances for getting or increasing your security budget/investments.
5. Only about one fourth of organizations currently have some form of application security management system or maturity model. But over 40% are looking at this for the coming 12 months. So there might be a lot of activity in this area in the near future, and we hope one of our OWASP projects, openSAMM (Open Software Assurance Maturity Model), can help executives with that.

Beyond these points, you will find this report contains many more interesting facts and findings and we hope that you will find many of them interesting and helpful for your daily work as a CISO, giving you the right data for defining your security strategies and priorities for the future. We are confident that like 2013, the coming year 2014 will be an interesting year with many challenges in web and application security and hope that we as OWASP can provide you and your organizations with good intelligence and help you with many of our free documentation and tools to manage your security programs better and overall improve application security around the world.

Introduction

Over the last years, we noticed that application security risks and threats have been on the rise and OWASP has started the CISO survey project to gather intelligence and provide it to CISOs and senior managers in order to improve their security strategies, assess their priorities and learn from their peers about what works best protecting web and application security in organizations across various industries. Although this first data set has already been collected from more than a hundred senior information security managers from around the world, to some degree the current data set was too small to be broken down into country or industry specific findings. Having said that, we found that on an anecdotal level, many of the findings appear to be consistent across a multitude of industries. OWASP will, in the coming year 2014, significantly further improve the breadth and depth of the current CISO survey and conduct it with a much wider audience around the globe.

A number of findings support common assumptions, but others clearly show where assumed general expectations have been oversimplified. The report provides insight into which risks and threats are on the rise, which challenges are most pressing for CISOs and their organizations and what techniques are particularly useful to counter application security risks.

The Survey methodology and data collection

The survey questionnaire consists of 26 comprehensive questions, across four domain areas:

- Investments and challenges,
- Threats and risks,
- Tools and technology,
- Governance and control.

The surveyed population mostly consists of:

- Chief Information Security Officers (CISOs)
- Senior security management

The population of surveyed CISOs was invited across a number of various CISO events, with a large portion of participants outside the common OWASP community. So we aimed at minimizing any OWASP specific biases, still, some small bias may remain as it is an OWASP project after all.

A good number of more than a hundred CISOs and senior security managers worldwide participated in this comprehensive survey.

Objectives

This report helps CISOs manage application security risks by considering the exposure from emerging threats and compliance requirements. This report helps:

- Make application security visible to CISOs and help them to make informed decisions on priorities and application security programs
- Provide strategic intelligence on which security risks are of the highest priority across organizations
- Provide tactical intelligence on best practices and free projects the CISO can leverage to improve their security programs.

Register to receive future updates and invitations for OWASP CISO projects

If you like to receive information about future releases of the OWASP CISO Survey and related CISO projects, you can register your email address here: https://docs.google.com/forms/d/1DBYIpWcx6IAZNHOXufdkLZKLIQXetwgbxxd7h_mqWN0/viewform

Your contact details will be kept strictly confidential and only used to send you updates about new releases of OWASP CISO projects and invitations to participate in the CISO Survey. And you can of course unsubscribe from this service at any time.

Questions and getting involved

If you have questions or like to actively support and participate in this project, please join the project mailing list https://www.owasp.org/index.php/OWASP_CISO_Survey_Project or feel free to send an email to the project lead at tobias.gondrom@owasp.org.

CISO Survey & Report 2013

The survey and report consist of four main building blocks.

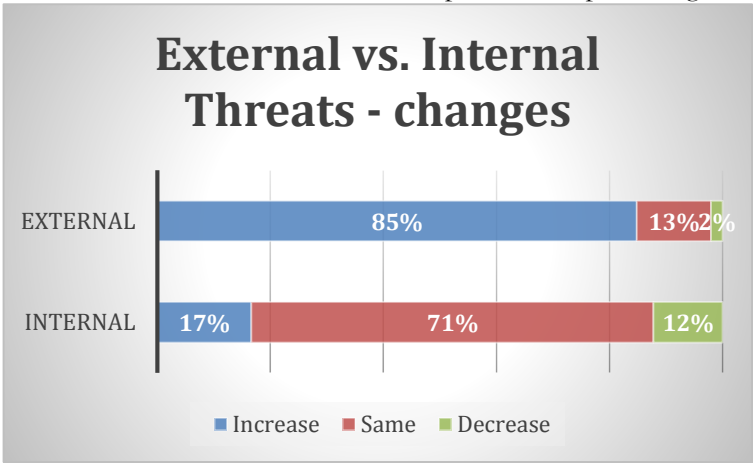
1. **Threats and risks**
2. **Investments and challenges**
3. **Tools and technology**
4. **Governance and control**

1. Threats and risks

As with all good security strategies, we were first interested in the trends of potential sources of security threats to organizations and how CISOs are addressing them.

External threats are on the rise

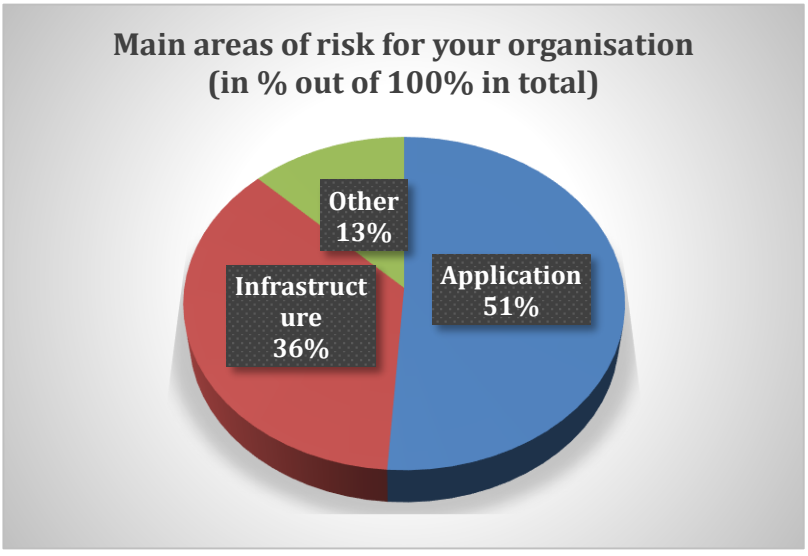
More than 70% of CISOs noted that internal threats are staying pretty much on the same level, while over 80% can see external threats clearly on the rise. It appears CISOs are more and more confident about their internal controls addressing internal security threats, like insiders stealing data or abusing systems. This can be due to a variety of reasons, better internal policies and controls and tools that enforce these policies and protect against malicious agents within an organization. While on the other hand, external threats seem to be increasing dramatically. This might be due to a variety of reasons: An increase in awareness due to more disclosures about security breaches by external sources, the fact that the IT systems of organizations are more and more exposed to the Internet and with that to external threat agents, an increased number of external malicious actors and potentially an upgrade in the skills and weaponized attack tools of potential attackers.



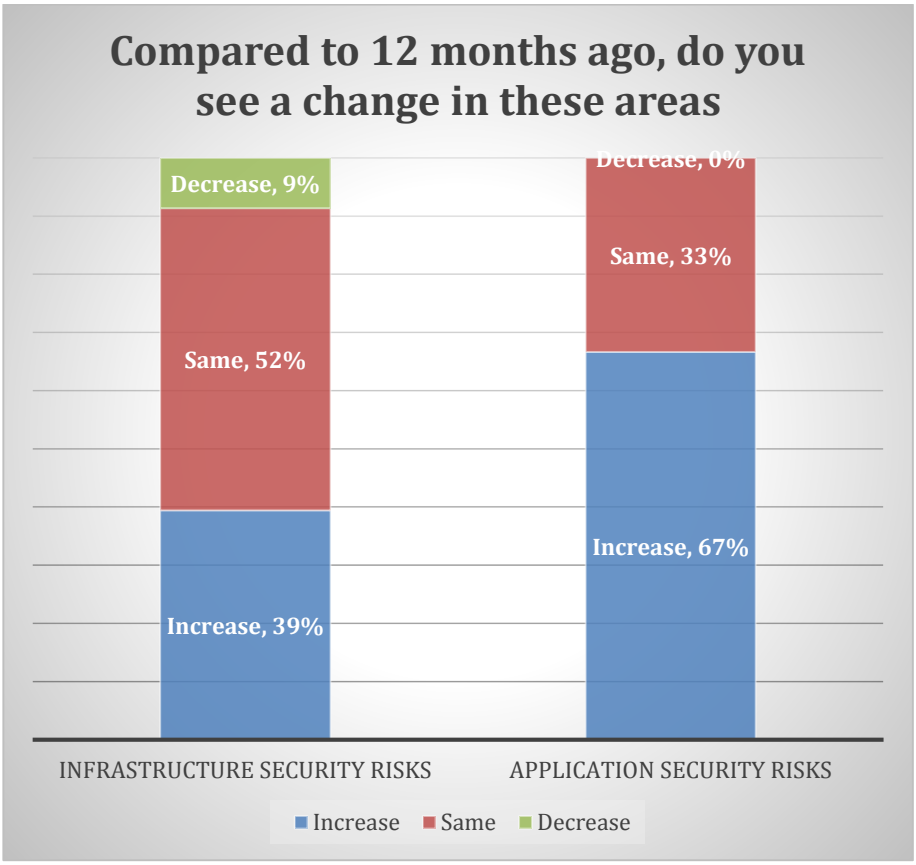
Application risks are advancing to center stage

When reviewing which areas are the main areas of risk for their organizations, CISOs were very clear that application security concerns are now taking center stage in their risk management. The CISOs see more than 50% of their security risks coming from application security:

The remaining 13% of "Other" were attributed to a mix of factors, in many cases to people centric risks and social engineering, but also to physical access controls and foreign states knocking on the door wanting critical data.

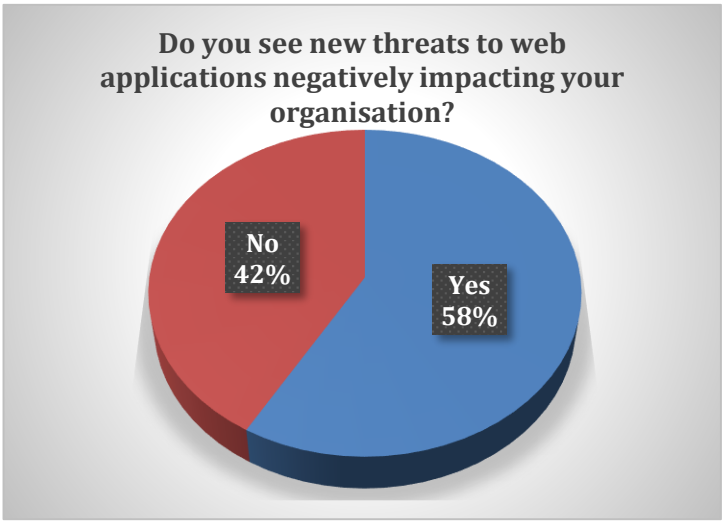


And furthermore, application security risks are increasing, while infrastructure issues are mostly stable.

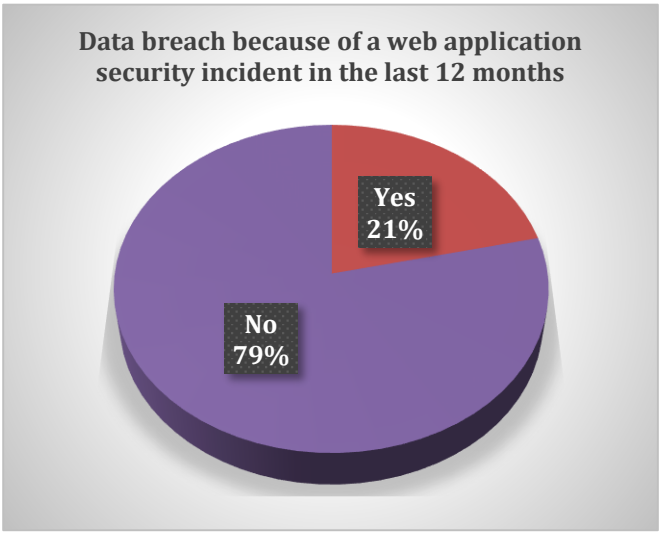


New threats to web applications are negatively impacting organizations

Based on the increase of application security risks, we were also wondering about their effects and whether organizations are seeing negative impacts from new threats to web applications. And the majority of CISOs could in fact clearly confirm that these threats are having negative impacts for their companies. Deeper discussions found that there are new threats due to technologies ranging from Social media, Web 2.0 and Cloud technologies like Software-as-a-Service, but also that attacks have increased in volume and sophistication, forcing companies to upgrade their security posture accordingly to counter more sophisticated attacks like spear-phishing, APTs, exposure of customer data and fraud.



Every fifth company experienced a security incident or data breach in the last 12 months.



About one in five of the companies did experience one or more data breaches because of a web application security incident in the last 12 months. To some degree this can be seen at odds with various other reports that have higher or lower percentages of security breaches. This may be due to different types of survey populations, e.g. more SMEs vs. large corporations, and also be accounted for by varying interpretations of the definition of an application security incident. However, even the figure of one in five companies having an application security incident or breach is a high risk, turning the focus of CISOs to application security risks.

Further analyzing these trends, we also asked CISO what they perceived as the top five sources of application security risks within their organizations. **Interestingly, a lack of budget for security initiatives came in only on the 4th place. The most pressing issue is the lack of awareness of application security issues within the organization.** A notion we find across a variety of questions and also reflected in the priorities for CISO going forward as you will discover in the following sections.

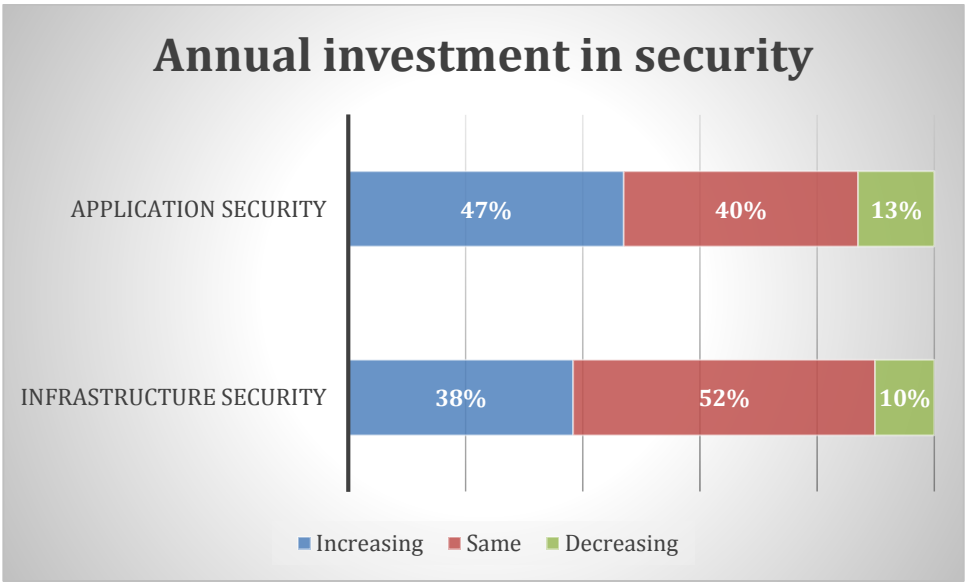
Top 5 CISO Application Security Risks

1. **Lack of awareness of application security issues within the organization**
2. **Insecure source code development**
3. **Poor/inadequate testing methodologies**
4. **Lack of budget to support application security initiatives**
5. **Staffing (e.g., lack of security skills within team)**

2. Investments and challenges

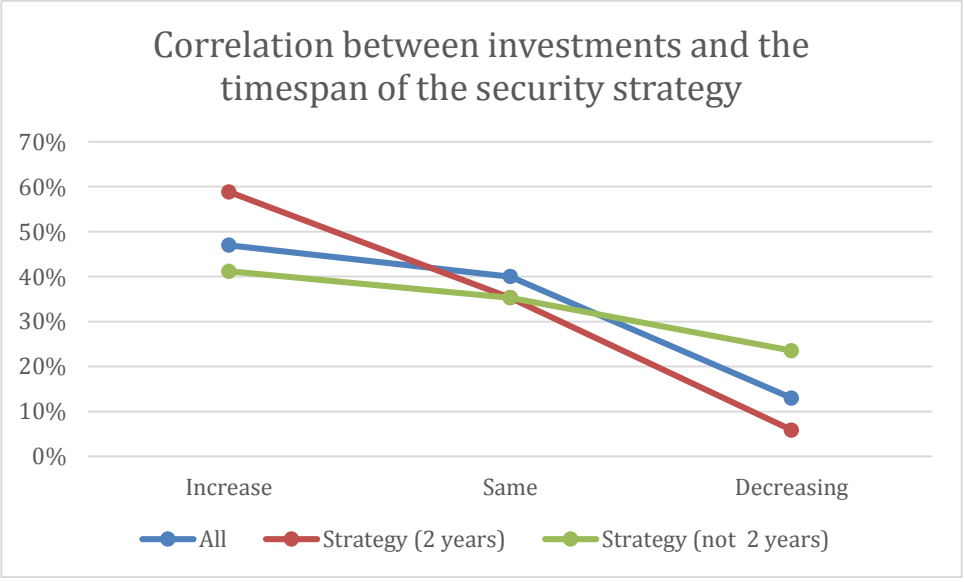
Increase of investments in Application Security

With regards to these risks and in general, application security investments are overall increasing for the next year, while the majority of budgets for infrastructure security will remain roughly the same.



Advantages of a two year application security strategy for budget allocations

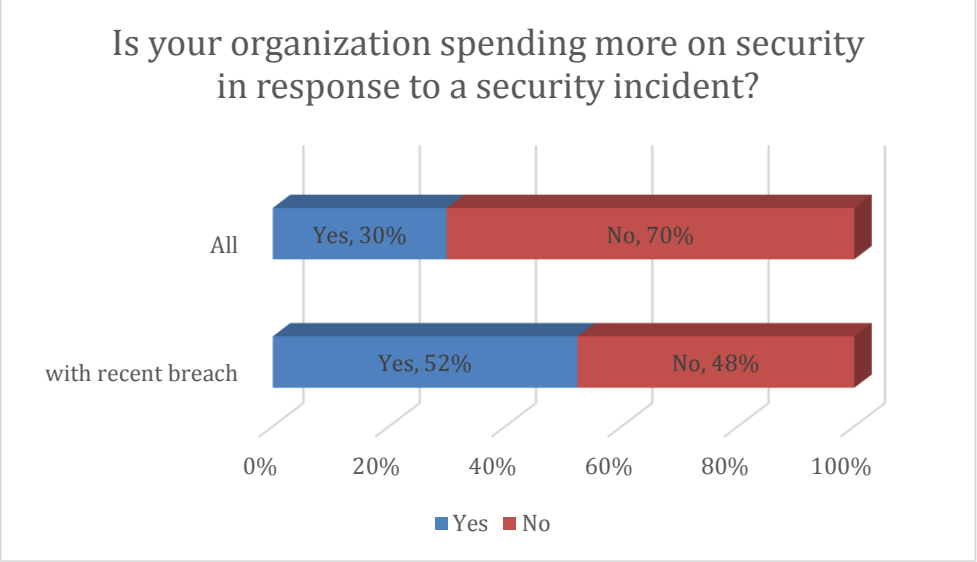
We also further analyzed the data for correlations of investments with a variety of factors, like whether an organization had a recent security breach, has an ASMS, company size, type of role of the submitting person (i.e. CISO), whether the organization has a security strategy, and the time horizon of the security strategy. So far we only found a significant correlation with the existence of 2-year security strategies. Other factors did not show a significant correlation, which can to some degree be due to the fact that the data set might not be large enough to prove other relationships.



Although of course correlation is not a proof for causality, it appears that there is a sweet spot of a 2-year security strategy that can help in budget decisions increasing investments in security. Other timespans did not show a significant improvement. Reasons behind this might be that a 2-year security strategy gives enough planning time to allocate security investments budgets into the following year, even if the budget for the current year is already exhausted. It may also give an advantage in the budget planning process to look beyond the annual budget plans. (More details about security strategies in the last section "Governance and Controls" and in part III of the OWASP CISO guide.)

We also wanted to analyze the influence of a previous data breach on new security investments. So far there have been frequent anecdotal reports that a recent breach can increase the motivation and chances of an organization to invest more in security. So we asked the CISOs about whether their organization would be spending more on application security in response to a breach or security incident related to a web application?

Nearly seventy percent stated that a recent breach would not influence their future spending in security. Interestingly this picture changes when you look at only the sub-group of companies who recently had an incident. There, more than half stated that they would increase spending on application security after an incident. Maybe going through the experience recently made them more aware for the potential turmoil and damages resulting from such breaches with the consequence of increased spending to not "get burned again". And vice versa, this could be an indication that companies who didn't recently suffer from a breach or an incident (or are not aware of it) might in fact be underinvesting in application security as they are underestimating the potential damages from such a security incident. It might also be an indication for a lack of proactive risk management strategy of some organizations when budgeting for the security of applications. As when the focus is on tactical risk management, a security incident may still trigger an increase in spending in application security even if is not considered a factor in the budgeting for a one or two year strategy.



The Top five application security priorities for the coming 12 months

After looking at the trends of application security investment, we analyzed deeper which specific areas CISOs identified as their Top-5 priorities for 2014. And we received as a clear Top priority the improvement of security awareness and training for developers, which corresponds well to counter the most important security risk as seen by CISOs, the lack of awareness of application security issues within the organization.

In line with these CISO priorities, OWASP will focus especially on this and has defined the improvement of security trainings as one of our key strategic goals for 2014.

Top 5 CISO Priorities

1. **Security awareness and training for developers**
2. **Secure development lifecycle processes (e.g., secure coding, QA process)**
3. **Security testing of applications (dynamic analysis, runtime observation)**
4. **Application layer vulnerability management technologies and processes**
5. **Code review (static analysis of source code to find security defects)**

Biggest challenges to effectively delivering your organization's application security initiatives

Interestingly the top challenge for CISOs is not acquiring adequate budget, but finding the right qualified resources and achieving awareness across the organization, be it among the developers who build new applications or the management team.

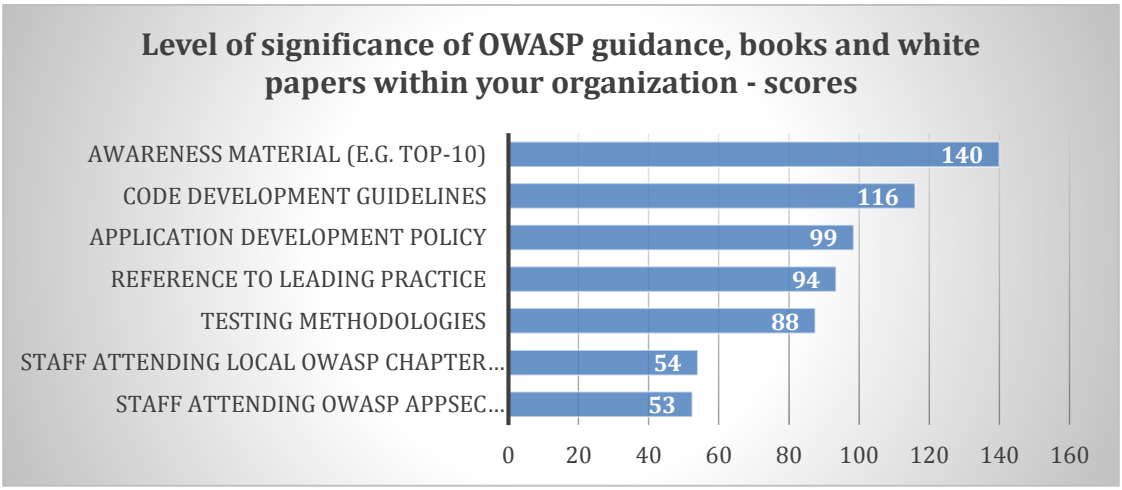
Top 5 CISO Challenges to effectively delivering your organization's application security initiatives

1. **Availability of skilled resources**
2. **Level of security awareness by the developers**
3. **Management awareness and sponsorship**
4. **Adequate budget**
5. **Organizational change**

3. Tools and technology

Significance of OWASP guidance, books and white papers

To better understand how organizations benefit from existing OWASP activities and what is most useful for organizations, we also asked the CISOs what OWASP activities serve them well, and which ones are more or less significant. For data analysis we designed a weighted scoring that would rank based on how many rated activities as extremely significant, very significant, significant, somewhat significant or not significant. Most significant help are OWASP projects for awareness programs and awareness material, with a weighted score of 140 and about 70% stating that OWASP is extremely significant, very significant or significant for this area. While staff attending local chapter meetings or AppSec conferences is still important, with a score of 54 and more than 30% of the surveyed CISOs rating this activity as extremely significant, very significant or significant.



Top-5 most useful OWASP projects for organizations from the perspective of the CISO.

The 5 most useful OWASP projects from the standpoint of a CISO are the

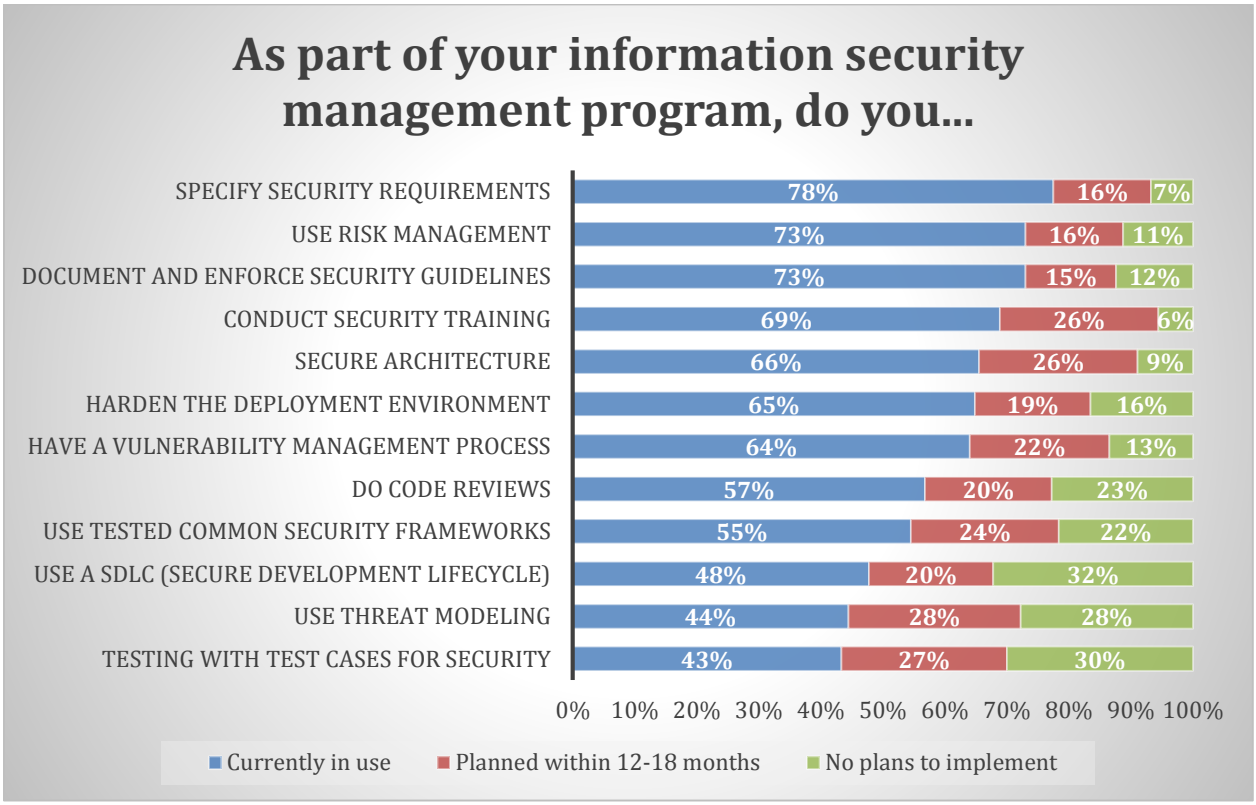
1. OWASP Top-10
2. Cheatsheets
3. Development Guide
4. Secure Coding Practices Quick Reference
5. Application Security FAQ

With the Top-10 a clear leading number one position, while the other four projects are relatively equal in their rating and basically sharing second place.

Top-5 most useful OWASP projects

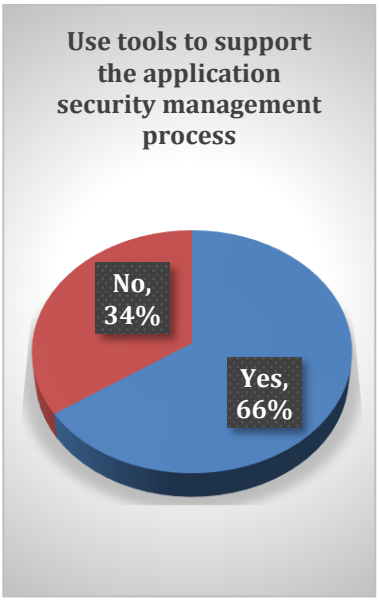
Design of the information security management program

As information security programs vary widely across organizations, we asked the CISO which key elements are part of their programs:

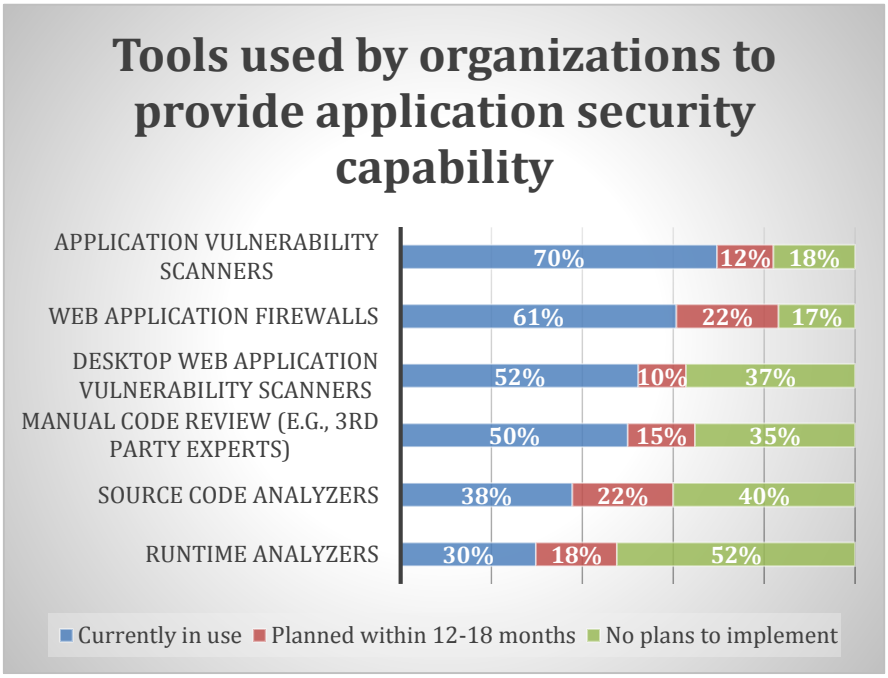


Naturally, security requirements, guidelines, security training and risk management were prevalent parts of information security management programs. Interestingly, using a secure software development lifecycle did rank fairly low as a part of the CISOs' current security management programs. This finding might also be an indication for a lack of using an application security strategy or maturity model to determine which domains to focus on and which SDLC activities to implement. (See also the OWASP CISO guide Part III : Application Security Program.)

Two thirds use technical tools to support their application security management process



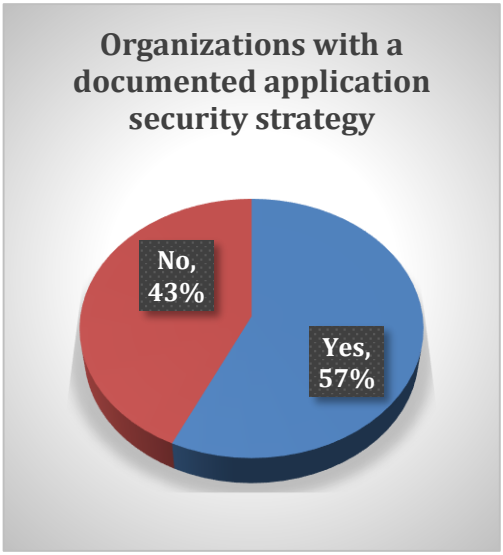
For example, we found the following tools are used by organizations:



4. Governance and control

Security Strategy

Noteworthy, although two thirds of organizations are using technical tools to support their programs, only about 57% have a documented application security strategy to guide their program decisions.



The median of security strategy timespans lies at 1 year, with about half of the organizations with security strategy timespans of 1 year or less and the other half with 2 years or more. As noted in the section on investments, interestingly we noted that there appears to be a correlation "sweet spot" for increasing your security budget if you use a planning horizon of two years (but note, we did not see additional budget advantages when going beyond the 2 years horizon.).

Duration	*Percentage*
3 months	10%
6 months	8%
1 year	35%
2 years	28%
3 years	12%
5+ years	7%

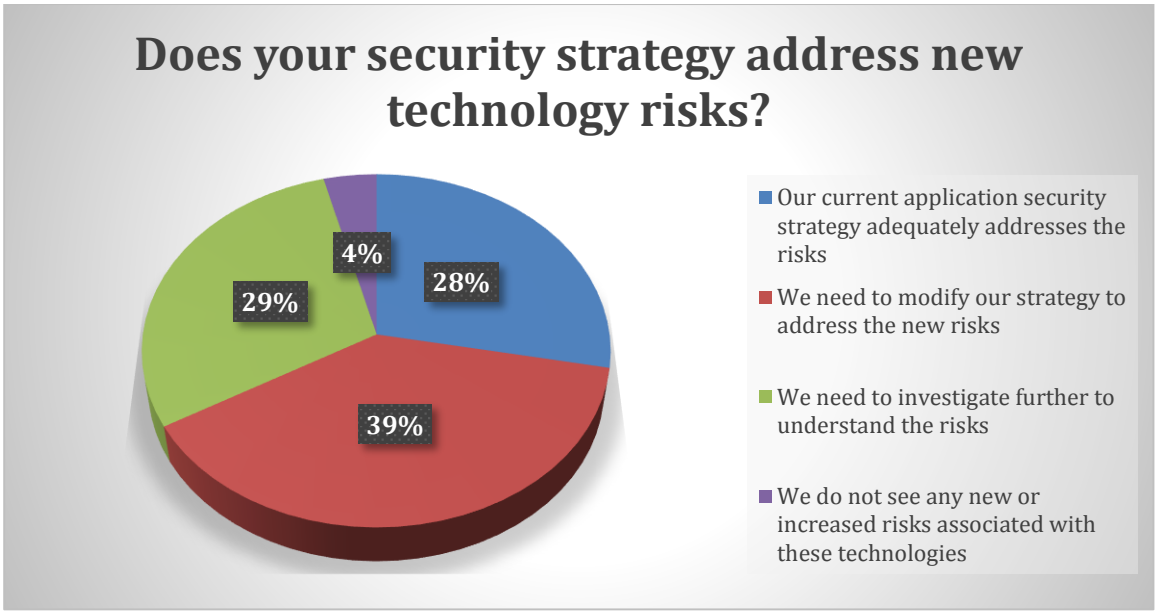
Alignment and review of the security strategy

An interesting observation is further: although the far majority have reviewed and updated their strategy within the past 12 months, yet, only half of the security strategies are aligned or integrated with the organization's business strategy and only half outline the key security activities for the next 12 months. Considering that CISOs see as one of their challenges an awareness gap of senior management for security topics, it might be a good idea to build that bridge from both ends: sharpen awareness for security issues and also at the same time align the security strategy with the business strategy, thus making it more relevant for day-to-day business decisions.

And of those with an application security strategy, this strategy	
… has been reviewed and updated within the past 12 months	76%
… is aligned with, or integrated into, the organization's IT strategy	65%
… is aligned with, or integrated into, the organization's business strategy	53%
… outlines our key security activities for the next 12 months	51%

Do strategies address new technology risks, related to social networking, personal devices, or cloud?

The question is not only whether your strategy is up-to-date and aligned with your business strategy, but there are constantly new risks arising and we asked CISOs how confident they are that their current strategy is addressing new risks associated with the increased use of social networking, personal devices, or cloud. And only one third found their strategy sufficient, while two thirds either need to investigate or modify how these new technology risks affect their security and security strategy.



Use of Application Security Management Systems (ASMS) and Maturity Models

We also noted that only a small portion of CISO are currently using an ASMS or maturity models to assess their security status and develop their security roadmap or strategy based on that assessment. In fact **only one in four** is using or in the process of currently implementing an ASMS.

Has your organization implemented an Application Security Management System (ASMS) or Maturity Model (e.g., OWASP SAMM)?	
Yes, implemented and formally certified/verified	5%
Yes, without verification	9%
Yes, currently in the process of implementing	12%
No, but considering it	41%
No, and not considering it	33%

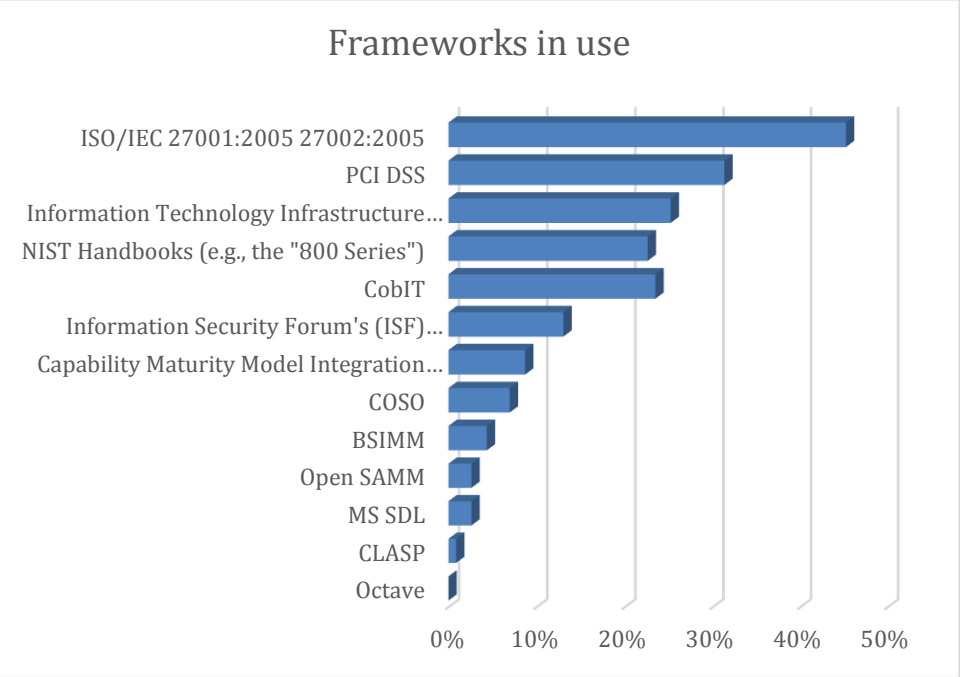
26%

This is interesting, as some may argue that it is vital to understand your current position in order to formulate an adequate security strategy going forward. However, ASMS and maturity models come in many different shapes and sizes and some of them can require great effort just for getting this first assessment.

(On a personal note: I found the OWASP openSAMM a very fast and lightweight maturity model to get that first assessment with a just few hours on an afternoon with some of my CISO clients. And building on that you can develop your security roadmap very quickly. And you may notice that openSAMM is still used in only very few organizations as you can see from the following graph.)

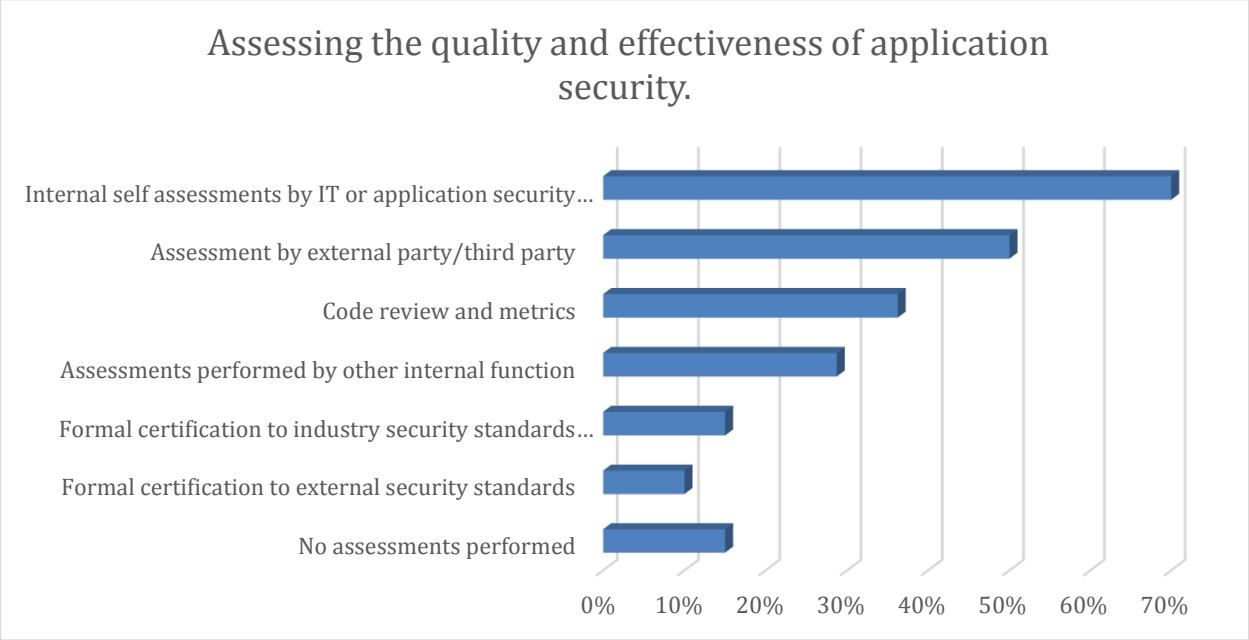
Frameworks and Security Management Systems used by organizations

Going beyond the maturity models, we also wanted to see which systems are used at the moment by organizations. And clearly the ISO 2700x standards are most common, used by nearly half of the organizations. But using a maturity model seems today to be still an exotic approach, practiced by only a minority.

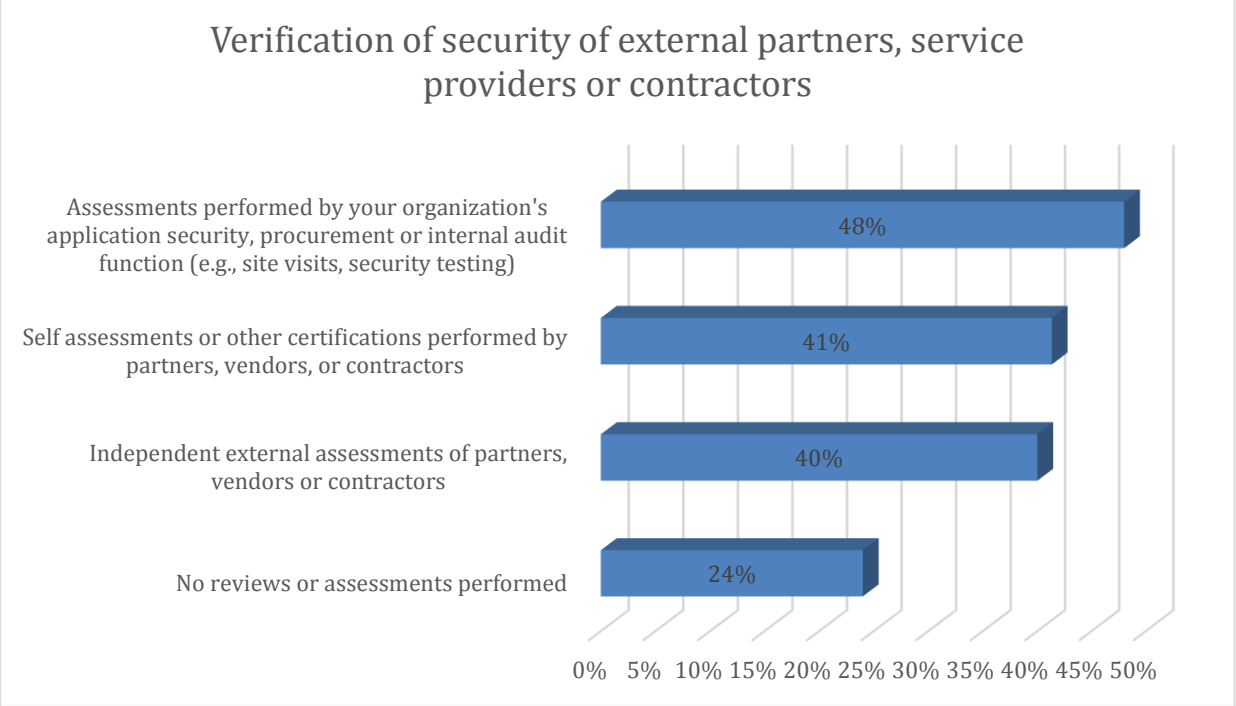


Assessing the quality and effectiveness of application security

And although the use of external frameworks is relatively low, the **vast majority (85%)** of organizations are performing assessments of their application security in one way or the other. Most of them through internal self-assessments by IT or application security functions.



Assessment of external partners, service providers and contractors



The CISO role: scope and areas of responsibility

And last but not least, we also took a closer look at the role and responsibilities of the CISO. They seem to still vary a great deal between organizations and across industries. So we were curious as to the current extend of the surveyed CISOs areas of responsibility and especially as to how far her/his domain is stretching when it comes to application security related questions.

Interestingly while CISOs find policies and metrics close to their desk, nearly one third of the CISOs find secure development processes (SDLC) outside of their area of responsibility, and nearly one fourth of the CISOs have security training and awareness not in their area of responsibility. These aspects might be due to delegation to other application stakeholders and/or lower levels of functional management. They could also indicate a gap in aligning CISO responsibilities on application security within risk management, governance and compliance. It will be interesting to see whether the CISO role will further evolve over time when revisiting the CISO role and responsibilities in the next iteration of the CISO survey in 2014.

CISO Functions & Responsibilities: areas of responsibility	
Investigate and analyze suspected security incidents and data breaches and recommend corrective actions	89%
Develop and implement policies, standards and guidelines for application security	86%
Measure and monitor security and risks of web application assets within the organization	86%
Work with executive management, business managers and internal audit and legal counsel to define application security requirements that can be verified and audited	83%
Network Security and perimeter defense	83%
Define, identify and assess the inherent security of critical web application assets, assess threats, vulnerabilities, business impacts and recommend countermeasures/corrective actions	80%
Application security training and awareness for information security and software development teams	77%
Develop, articulate and implement risk management strategy for applications	77%
Application Vulnerability Management	71%
Develop and implement software security activities (e.g. S-SDLC) and security testing processes	63%
Develop implement, manage and report on application security governance processes	60%
Procure new web application processes, services, technologies and testing tools for the organization	57%
Develop, articulate and implement continuity planning/disaster recovery for web applications	54%

Conclusions

Due to the evolving threat landscape and increased pressure from audit, legal and compliance, in the last decade, investments in application security have been a growing proportion of overall information security and information technology budgets. In our 2013 OWASP CISO Survey, nearly 90% of respondents indicated that application security investment would either increase or remain constant. Nevertheless, making the business case for increasing the budget for application security remains today one of many challenges of a CISO and security manager, because of competing objectives like the prioritization of spending for development of new application features and platforms (e.g. mobile devices), initiatives to expand service uptake or profitability, and marketing to attract new customers and retain existing customers.

In today's economic climate and ever changing threat landscape, it is increasingly important for CISOs to formulate the right security strategies for their organizations and articulate the "business case" for investment in application security and focus on the programs that have the most impact on the overall security of the organization and reducing risks.

That means, that today's CISOs need to navigate and master many challenges, the most pressing among them are: developing the right security skills within their organizations, achieving awareness for security risks among their developers and management teams, managing with limited budgets and adjusting to constant organizational changes. And in turn these challenges shape the key priorities for CISOs for the near and medium future: to improve awareness and training, transfer security awareness into program execution and budgeting, introduce or improve their secure development lifecycle and overall strengthen application security across the system landscape to counter the dramatically increasing external threats to application security.

When comparing the new data with spending reports, there also appears to still be a disconnect between organization's perceived threats of rising application security threats on the one hand and a yet still large spending on network and infrastructure security in absolute and relative numbers. Typically, additional budget allocation for application security includes the development of changes in the application to fix the causes of the incident (e.g. fixing vulnerabilities) as well as rolling out additional security measures such as preventive and detective controls for mitigating risks of hacking and malware and limiting the likelihood and impact of future data breach incidents. Still, even with limited budgets, CISOs can improve their security posture by focusing on the most critical risks of an organization and leveraging commonly available best practices and free tools to strengthen their organization and systems.

From a fear perspective – leveraging security incidents - it is true that CISOs can also exploit the momentum, being this either a negative or positive event. But this is part of a reactive risk management approach looking backward at past events and low maturity in dealing with future risks. Often application security spending can be triggered by a negative event such as a security incident, since this shifts senior management's perception of risk. However, CISOs should find that using a two year roadmap to drive security investment would be more effective in setting the appropriate security budgets.

In the case of experienced security breaches or incidents, the money is probably being spent to limit the damage, such as to remediate the incident and implement additional countermeasures. The main question then is what further investment in application security will reduce the likelihood and impact of another similar incident happening in the future. One approach is to focus on applications that might become a target for future attacks.

To help developing a more forward looking security strategy, many organizations will be looking at introducing application security management systems and/or maturity models over the coming 12 months. A trend that will allow organizations to further grow in maturity and improve their understanding of the security risks they are facing and how to best allocate their limited resources.

Concluding, we hope the sister project, the OWASP CISO Guide, can help the CISO with practical guidance on how to deal with many of these key findings and to decide the right security investments and strategies for their organizations going forward.

Register to receive updates: OWASP is planning a new CISO survey and report in 2014

If you like to receive future releases of the OWASP CISO Survey and related CISO projects, you can register your email address here:
https://docs.google.com/forms/d/1DBYIpWcx6IAZNHOXufdkLZKLIQXetwgbxxd7h_mqWN0/viewform

Your contact details will be kept strictly confidential and only used to send you updates about new releases of OWASP CISO projects and invitations to participate in the CISO Survey. And you can of course unsubscribe from this service at any time.

References

[1] Application Security Guide For CISOs
https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

[2] openSAMM: OWASP's Open Software Assurance Maturity Model
https://www.owasp.org/index.php/Software_Assurance_Maturity_Model

About OWASP

Description of OWASP

OWASP is a global open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. OWASP builds documents, tools, teaching environments, guidelines, checklists, and other materials to help organizations improve their capability to produce secure code. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.

OWASP was formed in 2001, in an entirely organic fashion, when a group of security professionals came to realize how terribly insecure the way we develop our web applications was. The initial goal was deemed to be modest: write a guide for developers, which would document secure software development practices. While the initial effort was meant to last a few weeks, it came out to several hundred pages. When released, the OWASP Guide to Building Secure Web Applications was an instant success. The OWASP Guide Series now encompasses six documents.

OWASP is a place where good people gather to help increase the awareness of the security problems in applications. It is a grass-roots effort, with the driving force being the people who are dealing with these problems every day, and wanting to lend a hand to change the situation for the better. The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success.

The OWASP Foundation is a US 501(c)(3) not-for-profit organization. OWASP Europe VZW is a non-profit organization registered in Belgium.

Participation

Everyone is welcome to participate in our forums, projects, chapters, and conferences. OWASP is a fantastic place to learn about application security, to network, and even to build your reputation as an expert. All OWASP's documents, tools and other resources are published using open source licenses, and are available free of charge.

Local Chapters

OWASP has almost 200 local chapters around the world. Chapter meetings are always free to attend, are vendor neutral and the presentations are made available free-of-charge on each chapter's web page. The meetings help foster local discussion of application security around the world.

To find your nearest local chapter, information on how to start a new one, and how to run a chapter see https://www.owasp.org/index.php/OWASP_Chapter and https://www.owasp.org/index.php/Chapter_Leader_Handbook

AppSec Conferences

For the last ten years, OWASP AppSec conferences bring together industry, government, security researchers, and practitioners to discuss the state of the art in application security. Global AppSec conferences are held annually in North America, Latin America, Europe, and Asia Pacific. Additionally, regional events are held in locations such as Brazil, China, India, Ireland, Israel, and Washington D.C. Presentation slides and video recordings are available free of charge on the OWASP website after each conference.

For upcoming global and regional events see
https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference

Citations

To find almost 80 national and international Legislation, standards, guidelines, committees and industry codes of practice that refer to OWASP see https://www.owasp.org/index.php/Industry:Citations

Helping to Support OWASP's Mission

Many organizations have been corporate or education supporters. many more are encouraging their employees to participate and contribute time and resources to OWASP Projects.

OWASP has also produced six guidance documents for other groups, suggesting how they could best support OWASP's mission. These are known as the OWASP Application Security Codes of Conduct, for government bodies, educational institutions, standards groups, trade organizations, certifying bodies, and development organizations. The Codes of Conduct can be downloaded from the project page
https://www.owasp.org/index.php/OWASP_Codes_of_Conduct

Contact

Our global address for general correspondence is:

FAO Kate Hartmann

OWASP Foundation

1200-C Agora Drive, #232

Bel Air, MD 21014

United States

The European correspondence address is:

OWASP Europe VZW

Leinstraat 104A

B-9660 Opbrakel

Belgium

Or phone Kate Hartmann at +1 301-275-9403 or use the contact form at http://sl.owasp.org/contactus

Appendix

Appendix A: Quick Reference of CISO domains to OWASP Guides & Projects

(from the appendix of OWASP CISO Guide [1])

This quick reference maps typical CISO's functions and information security domains to different sections of the OWASP' CISO Guide and relevant OWASP projects.

Table 1 CISO FUNCTIONS MAPPED TO OWASP GUIDES AND OTHER PROJECTS

CISO Function	Security Domain	OWASP CISO Guide	OWASP Projects
Develop and implement policies, standards and guidelines for application security	Standards and Policies	I-3 "Information Security Standards, Policies and Compliance"	• Development Guide - Policy Frameworks • Project CLASP - Identify Global Security Policy • Project SAMM - Policy & Compliance • Code Review Guide - Code Reviews and Compliance
Develop, implement and manage application security governance	Governance	III-3 "Application Security Governance, Risk and Compliance"	• Project SAMM - Governance • Project ASVS - How to Write Job Requisitions
Develop and implement software security development and security testing processes	Security Engineering Processes	III-4 "Targeting Software Security Activities and S-SDLC Processes" III-5 "How to Choose the Right OWASP Projects and Tools For Your Organization"	• Development Guide • Code Review Guide • Secure Coding Practices • Testing Guide • Comprehensive Lightweight Application Security Process (CLASP) Introduction • CLASP Concepts • Software Assurance Maturity Model (SAMM) • Testing Guide - Tools • Project Application Security Verification Standard Project (ASVS)
Develop, articulate and implement a risk management strategy for applications	Risk Strategy	I-4 "Risk Management Strategies" II "Criteria for Managing Application Security Risks" III-4 "Security Strategy"	• SAMM - Strategy & Metrics • Application Threat Modeling - Risk Mitigation Strategies
Work with executive management, business managers and internal audit and legal counsel to define application security requirements that can be verified and audited	Audit & Compliance	I-3 "Capturing Application Security Requirements" III-3 "Addressing CISO's Application Security Functions"	• Application Security Verification Standard • CLASP - Capture Security Requirements • SAMM - Security Requirements • Testing Guide - Security Requirements Test Derivation • Project OWASP Cornucopia • Project Secure Software Contract Annex
Measure and monitor security and risks of application assets within the organization	Risk Metrics & Monitoring	IV "Metrics for Managing Risks & Application Security Investments"	• CLASP - Define and Monitor Metrics • SAMM - Strategy & Metrics • Types of Application Security Metrics

CISO Function	Security Domain	OWASP CISO Guide	OWASP Projects
Define, identify and assess the inherent security of critical application assets, assess the threats, vulnerabilities, business impacts and recommend countermeasures/corrective actions	Risk Analysis & Management	I-4 "Risk Management" II "Criteria for Managing Application Security Risks"	• Project Top Ten Web Application Risks • Project Top Ten Mobile Application Risks • Project Top Ten Cloud Risks • ASVS - Implementation of NIST Risk Management Verification Activities • Risk Rating Methodology • Threat Risk Modelling • Application Threat Modelling
Assess procurement of new application processes, services, technologies and security tools	Procurement	III-4 "Assess Risks before Procurement of Third Party Components/Services"	• Project Secure Software Contract Annex • ASVS - Verification of Contract Requirements
Oversee the training on application security for development, operational and information security teams	Security Training	III-5 "People, Processes and Technology"	• Project CLASP - Institute Awareness Programs • Education Projects • Appsec Training Videos • Conference Videos • Application Security FAQs • CLASP - Institute Security Awareness Program
Develop, articulate and implement continuity planning/disaster recovery	Business Continuity / Disaster Recovery	III-3 "Addressing CISO's Application Security Functions"	• Cloud Business Continuity and Resiliency
Investigate and analyse suspected and actual application security incidents and recommend corrective actions	Vulnerability Management & Incident Response	I-4 "Addressing the Business Concerns after a Security Incident"	• SAMM Vulnerability Management • CLASP - Manage Security Issue Disclosure Process • .NET Incident Response

Appendix B: References to selection of OWASP Guides and Projects

- Application Security FAQs
  https://www.owasp.org/index.php/OWASP_Application_Security_FAQ
- Application Security Verification Standard (ASVS) Guide
  https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- Application Threat Modeling
  https://www.owasp.org/index.php/Application_Threat_Modeling
- AppSec Training Videos
  https://www.owasp.org/index.php/OWASP_Appsec_Tutorial_Series
- CLASP
  https://www.owasp.org/index.php/Category:OWASP_CLASP_Project
- Cloud Business Continuity and Resiliency
  https://www.owasp.org/index.php/Cloud-10_Business_Continuity_and_Resiliency
- Code Review Guide
  https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- Conference videos
  https://www.owasp.org/index.php/Category:OWASP_Video
- Cornucopia
  https://www.owasp.org/index.php/OWASP_Cornucopia
- Development Guide
  https://www.owasp.org/index.php/Category:OWASP_Guide_Project
- Education projects
  https://www.owasp.org/index.php/Category:OWASP_Education_Project
- .NET Incident Response
  https://www.owasp.org/index.php/.NET_Incident_Response
- Risk rating methodology
  https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- SAMM
  http://www.opensamm.org/
- Secure Coding Practices
  https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
- Secure Software Contract Annex
  https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex
- Testing Guide
  https://www.owasp.org/index.php/OWASP_Testing_Project
- Threat risk modeling
  https://www.owasp.org/index.php/Threat_Risk_Modeling
- Top Ten Cloud Risks
  https://www.owasp.org/index.php/OWASP_Cloud_%E2%80%90_10/Initial_Pre-Alpha_List_of_OWASP_Cloud_Top_10_Security_Risks
- Top Ten Mobile Application Risks
  https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks
- Top Ten Web Application Risks
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Types of Application Security Metrics
  https://www.owasp.org/index.php/Types_of_application_security_metrics