MARKET RESEARCH

SECURE CODING

SECURE CODE
WARRIOR

Content

Introduction

Even those active in software industry tend to forget about the fact that the burden of the security incidents we experience today are stemming from defects in the code – actually bugs – committed by software engineers designing, implementing and integrating IT systems. This is not surprising, as software security practices are usually not even included in standard programming courses.

Constrained by resources, many software vendors ignore security entirely until they face any incidents, or are tackling security by just focusing on the options they think to be the cheapest – which usually means post-incident patching and automatic updates. Software security, however, has to be applied holistically: without seeing the big picture, one cannot stop hackers and attacks effectively.

To date we have learned the lesson: security started to be interwoven in the whole of the product development lifecycle from requirements specification, design and implementation to testing, deployment and operation. But do not forget: while engineers have to be vigilant and find every single bug in the code to make a product secure, for an attacker it is enough to find a single remaining vulnerability in a rarely-used module to use it as a vehicle for spamming, scamming or fraud. Based on over ten years of experience at helping vendors secure their software throughout the development lifecycle, our intention with this position paper is to illustrate and clear some of the misconceptions about software security.

Hacking is not anymore just an arcane activity committed by social outcasts with a strange hobby. There are well organized criminals who are gaining good money by taking over computers through attacking vulnerable software across the Internet, and creating botnets consisting of thousands or millions of zombie machines to do their bidding. This became big business, an industry on its own. Due to the effective financial motivation, attackers are coming up with newer attack methods literally every day. Just a decade ago we mainly had to deal with buffer overflows, and by now we have learned how to protect against them.

But the landscape is continuously changing; new technologies appear regularly, usually solving some known problems, but – most of the time – they also introduce new ones. This is an eternal cat-and-mouse game. The landscape of motivations also changes. From cyber-crime we are apparently moving towards cyber-war and cyber-terrorism these days, with major players expending massive resources, resulting in much more severe consequences that we are yet to experience.

Stuxnet, Duqu and Flame are examples of complex malware developed by – usually government-supported – security specialists for millions of dollars that can destroy factory machinery or spy on targeted victims while being undetectable for long enough to do the job. Yet even these are doing nothing else but exploiting security vulnerabilities – actually: bugs – being present in software products.

Similarly, an aggregation of some common security-relevant bugs and flaws in Sony's PlayStation Network service caused a widespread loss of confidential user data, and a month-long outage of the entire service. Sony suffered $170 million dollars of losses, and an 8% drop in the company's stock price in a week. Companies that had faced a successful attack started to spend more on security than before, realizing that it is still the better overall option.

So vulnerabilities are here to stay. But several sources confirm – including CERT, SANS, Gartner or Microsoft – that around 90% of attacks do actually exploit well-known vulnerabilities, which have been already published at least six months before the attack took place[1]. So, usually we have solutions, but are not using them; just like driving cars without safety belts fastened.

Securing software is possible in many different ways, but not all approaches are equivalent in efficiency or usefulness. Before clearing up some misconceptions, let us put our two cents in the debate on some commonly misused terms. Security vs. safety – can you tell the difference? Did you know that some languages do not even have two distinct words for the two concepts? There are many attempts to give a good definition; the essential difference is however that in case of security we should always assume an intelligent actor who is willing to attack you; in case of safety it’s all about Mother Nature and bad luck.

People also often conflate software security with IT security. This latter is actually much broader, focusing on both organizational and technological aspects of information technology in general. As part of it, application security is about protecting the developed software after it has been deployed by applying techniques and tools to detect and prevent attacks and the exploitation of bugs; as opposed to this, software security covers the whole development lifecycle, and aims to prevent the occurrence of vulnerabilities during design, implementation and testing of the system – before it gets deployed.

Actually it is exactly about how to build secure software. Security testing is a challenging discipline that requires a fundamentally different mindset from functional testing. While functional testing consists of the verification of well-defined requirements, security testing involves finding evidence of abnormal operation in non-obvious borderline cases. To do effective security testing, one should be trained to have a solid expertise in security, be able to think as attackers do, and be aware of the testing methodologies, techniques (like fuzzing or fault injection) and tools.

But – just to repeat – in theory a security tester needs to find all the security-relevant bugs to secure a product, while for the attackers it is enough to find a single remaining vulnerability to perform an attack. Quite tricky. Security auditing, on the other hand, is a targeted assessment usually done by 3rd party professionals. While security testing searches for implementation problems in the entire product, an audit verifies that security controls in the product and the development process itself are properly implemented, and evaluates its overall security level.

Let us now turn to some commonly used approaches today, which are without doubt good practices. They are however not oracles – or silver bullets, as we call them in software security – but still, hyped as they are, people tend to believe that using these will solve it all. Compliance to requirements, standards, and best practices is inevitably something that will make a product more robust and resilient to attacks. These schemes provide a good checklist to go through which will improve security, but they tend to make developers think that they’ve done everything possible to protect their software.

[1] http://www.securecodingacademy.com/documents/10739/0/SW%20Security%20facts%20and%20misc%20WHITE%20PAPER

Some even say that compliance is killing “real” security by providing this confidence and a false sense of security. Ethical hacking sounds like a good thing to do, and it certainly is fun. But hacking – regardless whether it is done for a good or bad purpose – is ultimately about exploitation of vulnerabilities, which is a demanding and resourceful activity. Once a vulnerability is found as a result of security testing, analyzing how it can be exploited does not really make things any better.

Why not just fix it? Penetration testing – originally used for network security – is a practice of simulating attacks against deployed software products. Doing pentesting basically means going through a checklist of attack attempts, possibly supported by various automated security testing tools. It is – again – a good practice, but it alone will not provide an ultimate protection against all possible attacks.[2]

Why Train Developers? Assigning a security expert to a development project is a good idea for a start. But as even the smallest bug can compromise a system, the overall average preparedness of all involved software engineers – architects, programmers, testers – is the one that counts.

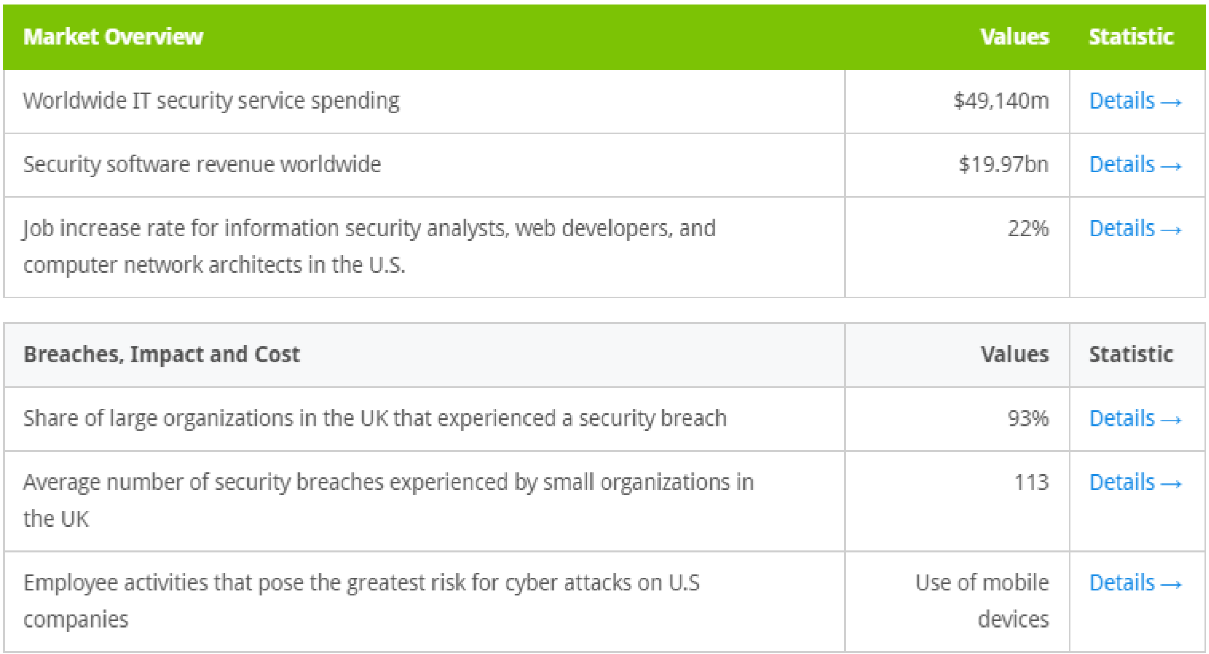
During the 2000’s the software industry started to realize that in the long run, investing in their own employees is the most cost-effective way of doing security. Training became the key preSDL requirement in the Microsoft Security Development Lifecycle, and companies started to reserve more and more from their security budget to educate their employees.

Education tackles the problem of security right at its source: the engineers. Teaching software security practices to corporate development groups needs a special prudence. The courses should be practical but still go into details; issues should be supported by exercises giving hands-on experience; and classes should be intensive so they don’t pull people away from their projects for too long.

[2] http://www.securecodingacademy.com/documents/10739/0/SW%20Security%20facts%20and%20misc%20WHITE%20PAPER

General stats

Statistics and facts about Information Security

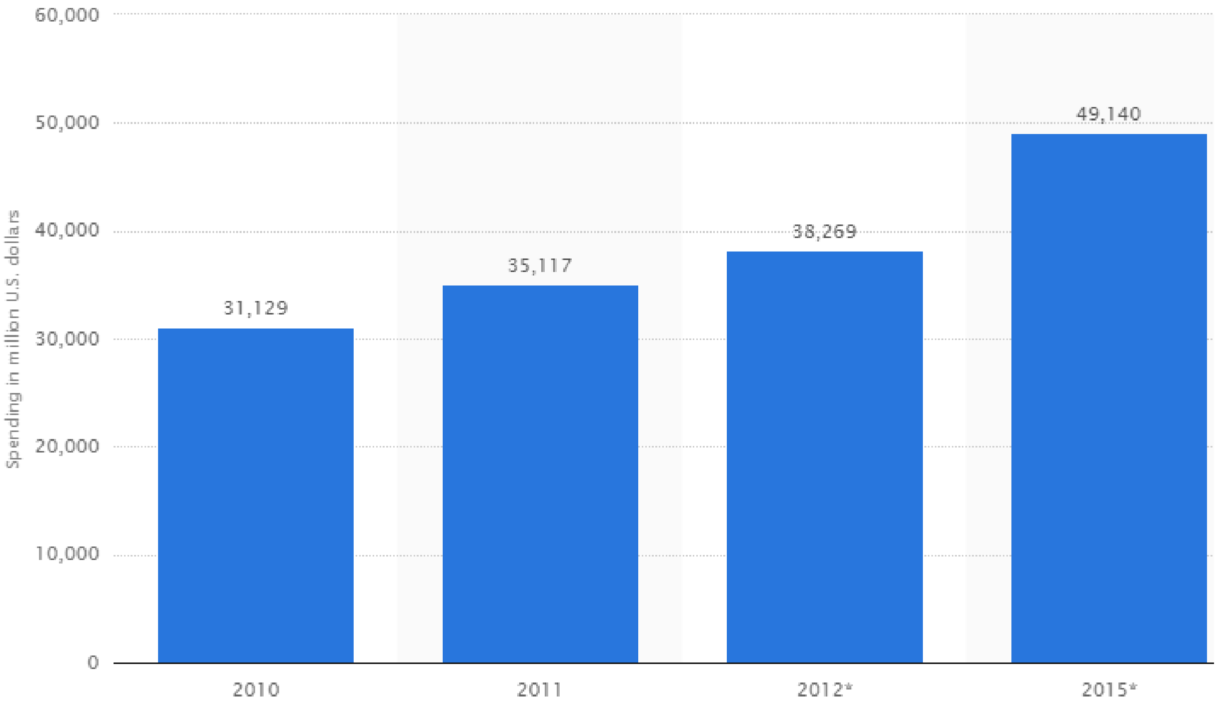


Market Overview	Values	Statistic
Worldwide IT security service spending	$49,140m	Details →
Security software revenue worldwide	$19.97bn	Details →
Job increase rate for information security analysts, web developers, and computer network architects in the U.S.	22%	Details →

Breaches, Impact and Cost	Values	Statistic
Share of large organizations in the UK that experienced a security breach	93%	Details →
Average number of security breaches experienced by small organizations in the UK	113	Details →
Employee activities that pose the greatest risk for cyber attacks on U.S companies	Use of mobile devices	Details →

Source: http://www.statista.com/

Worldwide IT security service spending from 2010 to 2015 (in million U.S. dollars)



Source: http://www.statista.com/

The statistic depicts the worldwide IT security service spending from 2010 to 2015. In 2015, the security service spending is projected to amount to 49,140 million U.S. dollars worldwide. In 2015, the security service spending in the consulting segment is projected to amount to 12,152 million U.S. dollars worldwide.

Gartner Stats - 2013[3]

As companies continue to expand the technologies they use to improve their overall security, the worldwide security technology and services market is forecast to reach $67.2 billion in 2013, up 8.7 percent from $61.8 billion in 2012, according to Gartner, Inc. The market is expected to grow to more than $86 billion in 2016.

Gartner analysts discussed the outlook for the security market at the Gartner Security & Risk Management Summit, being held here through Thursday.

"With security being one of the top IT concern areas, the prospect of strong continued growth is assured," said Ruggero Contu, research director at Gartner. "The consistent increases in the complexity and volume of targeted attacks, coupled with the necessity of companies to address regulatory or compliance-related issues continue to support healthy security market growth."

Gartner analysts see three main trends shaping the security market moving forward — mobile security, big data and advanced targeted attacks.

Bring your own device (BYOD) is a megatrend that will have a far-reaching influence on the entire security industry. Changes in how security addresses BYOD leaves several opportunities for technology service providers (TSPs). Firstly, with the shift from device security to app/data security there is a chance for some security TSPs to capture endpoint protection budgets. Secondly, since some BYOD projects are centered on the productivity gains of one to two apps, there could be buying centers adding security outside of traditional information technology centers. Finally, being able to understand the device type and how your users are computing today is just as important as who they are. An opportunity exists for those able to determine that context, and provide it for other points of influence, such as the network or applications.

The amount of data required for information security to effectively detect advanced attacks and, at the same time, support new business initiatives, will grow rapidly over the next five years. This growth presents unique challenges when looking for patterns of potential risk across diverse data sources. However, big data, in and of itself, is not the goal. Delivering risk-prioritized actionable insight is.

"To support the growing need for security analytics, changes in information security people, technologies, integration methods and processes will be required, including security data warehousing and analytics capabilities, and an emerging role for security data analysts within leading-edge enterprise information security organizations," said Eric Ahlm, research director at Gartner.

[3] http://www.gartner.com/newsroom/id/2512215

When examining the advanced targeted attack (ATA), and the new methods being used to breach today's security controls, it can be distilled to a basic understanding. Attackers, especially those who have significant financial motivation, have devised effective attack strategies centered on penetrating some of the most commonly deployed security controls (largely signature-based antivirus and signature-based intrusion prevention), most often by using custom or dynamically generated malware for the initial breach and data-gathering phase.

Advanced attackers are now capable of maintaining footholds inside an organization once they successfully breach security controls by actively looking for ways to remain persistent on the target organization's internal network. They do it either through the use of malware or, even if the malware is detected and removed, via postmalware use of user credentials gathered during the period of time the malware was active. They then change their tactics to secondary attack strategies as necessary, looking for other ways around any internal security controls in the event they lose their initial attack foothold.

"Mitigating the threat from ATAs requires a defense-in-depth strategy across multiple security controls," said Lawrence Pingree, research director at Gartner. "Enterprises should employ a defense-in-depth, layered approach model. Organizations must continue to set the security bar higher, reaching beyond many of the existing security and compliance mandates in order to either prevent or detect these newly emergent attacks and persistent penetration strategies. This layered approach is typical of many enterprise organizations and is often managed in independent ways to accomplish stated security goals, namely, detect, prevent, respond and eliminate."

Gartner Stats – 2014[4]

Worldwide spending on information security will reach $71.1 billion in 2014, an increase of 7.9 percent over 2013, with the data loss prevention segment recording the fastest growth at 18.9 percent, according to the latest forecast from Gartner, Inc. Total information security spending will grow a further 8.2 percent in 2015 to reach $76.9 billion.

According to Gartner, the increasing adoption of mobile, cloud, social and information (often interacting together) will drive use of new security technology and services through 2016.

“This Nexus of Forces is impacting security in terms of new vulnerabilities,” said Gartner research director Lawrence Pingree. “It is also creating new opportunities to improve effectiveness, particularly as a result of better understanding security threats by using contextual information and other security intelligence.”

Mr. Pingree said that the bigger trend that emerged in 2013 was the democratization of security threats, driven by the easy availability of malicious software (malware) and infrastructure (via the underground economy) that can be used to launch advanced targeted attacks.

[4] http://www.gartner.com/newsroom/id/2828722

"This has led to increased awareness among organizations that would have traditionally treated security as an IT function and a cost center," said Mr. Pingree.

Other trends in the information security market that form assumptions behind Gartner's latest forecast include[5]:

- ***By 2015, roughly 10% of overall IT security enterprise product capabilities will be delivered in the cloud.***

A significant number of security markets are being impacted by newly emerged delivery models. This is resulting in the growth of cloud-based security services, which are transforming, to different degrees, the way security is supplied and consumed by customers. While cloud-based services' competitive pricing puts pressure on the market, the cloud is also providing new growth opportunities, as some organizations switch from deploying on-premises products to cloud-based services or cloud-managed products. More than 30% of security controls deployed to the small or midsize business (SMB) segment will be cloud-based by 2015.

- ***Regulatory pressure will increase in Western Europe and Asia/Pacific from 2014.***

Regulatory compliance has been a major factor driving spending on security in the last three years, particularly in the U.S. Gartner expects this influence to accelerate from 2014. Broader data privacy legislation such as the Australian Privacy Act is expected to sustain spending on security this year. Other examples of intensifying regulatory pressure driving spending on compliance include the issue of guidelines regarding personal information protection in China in February 2013 (although they are not legally binding) and planned implementation of an addition to the EU Data Protection Directive. Other examples include personal data protection laws (introduced in 2013) in Singapore and Malaysia.

- ***By year-end 2015, about 30% of infrastructure protection products will be purchased as part of a suite offering.***

The presence of highly mature and commoditizing technologies, such as EPP and email security, will be contrasted by growth opportunities offered by segments such as SIEM, DLP and emerging technologies within the "other security" segment. Security providers in the more mature and consolidated segments are predicted to support sales through the addition of new security controls as part of broader suite offerings. This will be the case within the EPP segment, with the increasing availability of DLP, mobile device management, vulnerability assessment, hosted archiving and encryption for secure email gateway. This expansion of suite offerings to include new security controls is expected to help maintain momentum and slow down commoditization of these mature markets.

- ***By 2018, more than half of organizations will use security services firms that specialize in data protection, security risk management and security infrastructure management to enhance their security postures.***

[5] http://www.gartner.com/newsroom/id/2828722

Many organizations continue to lack the appropriate skills necessary to define, implement and operate appropriate levels of data protection and privacy-specific security controls. This lack of skills leads organizations to contract security consulting firms that specialize in data protection and security risk management to address regulatory compliance demands and enhance their security postures. A significant portion of organizations are shifting existing resources away from the operational aspects of security technologies, such as security device administration and monitoring, toward mitigation and incident response. This new dynamic has given rise to significant growth throughout the globe for managed security services.

- ***Mobile security will be a higher priority for consumers from 2017 onward.***

There is a lack of penetration of security tools among users of new mobile platforms, and Gartner does not expect to see new demand for this type of capability to emerge before 2016. Most consumers do not recognize that antivirus is important on mobile devices and therefore have not yet established a consistent practice of buying mobile device endpoint protection software. This purchasing trend and market shift away from PCs will have significant repercussions on the consumer security market. However, as mobile devices gain in mass popularity and as security is likely to be a higher priority from 2017 onward, then new market opportunities are likely to emerge.

It has not always been that way[6].

In 2002, I briefly abandoned the then information security market. Frankly, it sucked. I can remember more times than I care to admit saying, "This is just too hard." Or, "There's no money in information security." We all knew the problems for the solutions we were building existed, but back then, the market simply didn't care.

In 2002, the minimum standard of care for enterprises was limited to anti-virus, firewalls, intrusion detection, and, later, if you were in a regulated industry, SIEM or some sort of log aggregation solution. Enterprise executives lived in ignorant bliss, believing that their biggest risks were related to being out of compliance with their respective regulatory authorities.

In 2002, Gartner estimated the worldwide security software market to be an anemic $3.5 billion -- a market that was dominated by five vendors that owned approximately 60% marketshare -- Symantec , Network Associates, IBM, TrendMicro, and Check Point.

Fast-forward to 2014. New product categories abound, with Gartner covering too many cyber security-related magic quadrants to list (with more on the way). Investors are enthusiastically entering the market, with VCs investing $1.4 billion in 230 cybersecurity companies in 2013 alone.

So, what has fundamentally changed since 2002? What are the factors that are driving cyber security market growth? Here are four fundamentals that we at Mach37 continue to think about.[7]

[6] http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128

[7] http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128

First: The obvious. The threat continues to accelerate in capability and scale. Cybercrime is big business and has finally reached the tipping point where consumers and regulators are demanding that businesses deploy effective solutions.

Second: The Internet-of-Things is exacerbating the problem. Now, we have laptops, iPhones, wearable computers, gaming systems, other mobile devices… the list is boundless. Many of these devices are either themselves untrustworthy or are interacting with untrustworthy mobile networks. Few have the computing horsepower to perform traditional security functions of familiar desktops and laptops -- making them even easier targets. As difficult as the security problem was before, it just got a lot worse.

Third: Cyber security is now a Main Street issue. Every one of us is affected -- and now we finally realize it. Retail-related breaches, such as the recent Target breach, have hit tens of millions of consumers. Cyber security stories are now common in all mass media outlets.

Fourth: The competitive market is finally rewarding innovation. For many years, the information security market was dominated by large security platform companies that milked their antivirus cows and had very little incentive to innovate. Because of incumbent supply chain dominance, new entrants were often forced to battle over a very small number of early adopters or to sell to or through these powerful few to reach the broader market.

Over the past few years, new entrants have emerged and are challenging the fat incumbents… and the financial markets are rewarding them. As I write this, FireEye enjoys a market cap of $5.7 billion, with an astounding 35x (yes, I said 35) enterprise value to revenue multiple. Similarly impressive, although more modest, Palo Alto Networks trades at roughly 9x revenue with a $5 billion market cap.

Conversely, historical incumbent Symantec is trading at paltry 2x revenue and recently fired its CEO and executive management team.

I am sure there are many other factors, but whatever has changed in cyber security, the need for continued innovation has remained constant. Similarly, the fundamentals described above are not likely to change for at least a generation. And, speaking for those of us who lived through 2002, I am really glad to be in this market.

Future

Cyber attacks are like serious illnesses or job layoffs. We know they could happen to us at any given time, but we prefer to take the obvious precautions—and then try not to think about it.

Today, U.S. utilities are more vulnerable to hacking than ever before, as they upgrade to two-way, networked smart grids nationwide—and as the frequency and sophistication of cyber-mayhem increases globally.

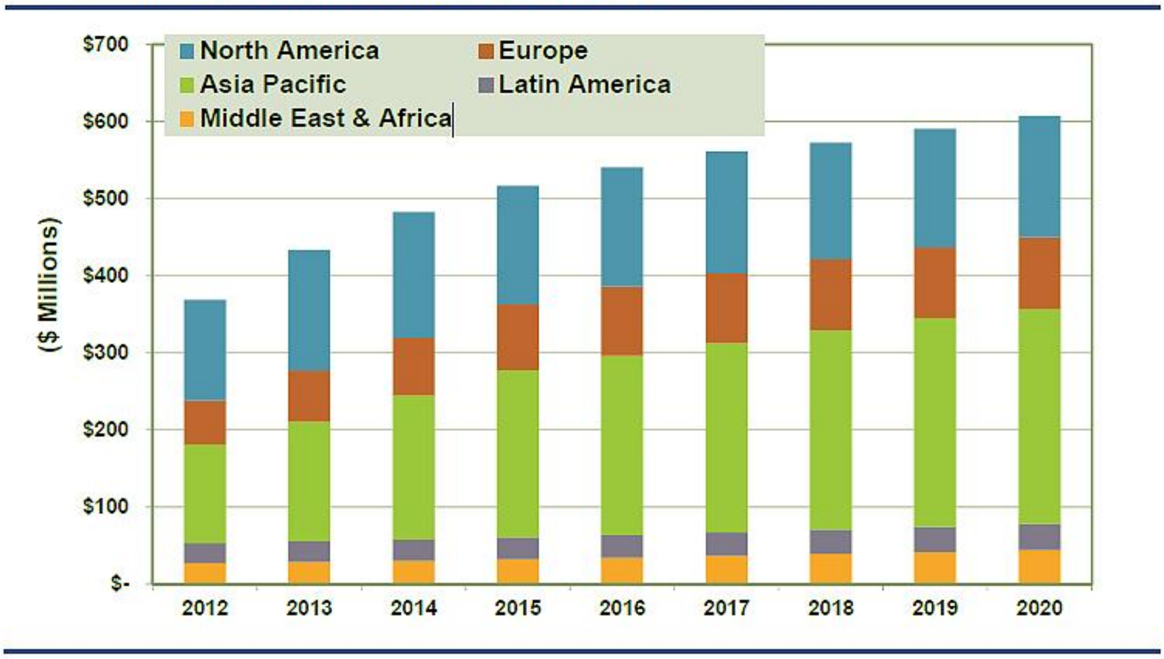
Discussions of security for smart grid industrial control systems (ICS) among utilities, vendors, systems integrators and public regulators have become more common in recent years, and utilities as a group appear to be better informed of cyber risks to their grids and substations.

But funding for these upgrades remains spotty, according to a recent report from Boulder, Colorado-based Navigant Research.

In the new study, “Industrial Control Systems Security,” Navigant ballparks the market for smart grid ICS cyber security at $608 million in 2020—expanding at a relatively slow compound annual growth rate of 6.4 percent, the study concludes.

“Utilities’ awareness of potential threats and risks to industrial control systems is growing, but utilities mainly view security as a method of limiting costs, and advances toward meaningful regulations remain weak,” commented Navigant Senior Research Analyst, Bob Lockhart. “Despite that discouraging overview, though, progress will be steady as the cost of complacency becomes more visible.”

Chart 1.1 *ICS Security Revenue by Region, World Markets: 2012–2020*



Source: http://smart-grid.tmcnet.com/topics/smart-grid/articles/2013/04/04/333033-smart-grid-cyber-security-faces-funding-challenges.htm

One sign of progress is the increasing number of utility cyber security consulting engagements. However, legacy systems often lack basic information about where devices are located and how they communicate with each other and the network—making security assessments difficult. In such cases, a pre-assessment initiative to map the network is required.

For utilities hoping to deploy one or two new products and declare victory, this can be disappointing news.

What’s more, vendor approaches to the market vary. Some strategically propose a full cyber security solution for an entire control network, with architecture and technology approaches to address every known threat and vulnerability.

Others take a more tactical approach and propose only to solve a specific problem, at least for the short-term.

In the end, the main obstacle to secure control systems is simply the will to allocate enough of a budget to achieve a secure environment. Despite the improved awareness, many utilities remain challenged to allocate security funding beyond that needed for compliance minimums. Navigant does not expect sufficient regulations to drive more spending within the next two to three years, but the uptick in professional services engagements encourages hope for growth in the near future.

US market

ASIS International (ASIS) and the Institute of Finance and Management (IOFM) jointly announce the release of "The United States Security Industry: Size and Scope, Insights, Trends, and Data," an extensive benchmark study of the private security industry's expansion over the past decade and projected future growth. An analysis of the security products and services market, as well as the industry's personnel market, is presented within the report. ASIS is the leading organization for security professionals worldwide. A business unit within Diversified Business Communications, IOFM is a renowned source of market intelligence and resources in physical security and corporate financial management.

Over 400 security industry executives participated in the United States Security Industry Survey, conducted in late 2012. A companion survey of security manufacturers and vendors, security services providers, dealers, distributors, installers and integrators was also conducted in order to enhance market projections. Information collected was analyzed, aggregated and combined with additional data from related national studies conducted by ASIS and IOFM, as well as publicly available information from U.S. government data and market research of homeland security spending.

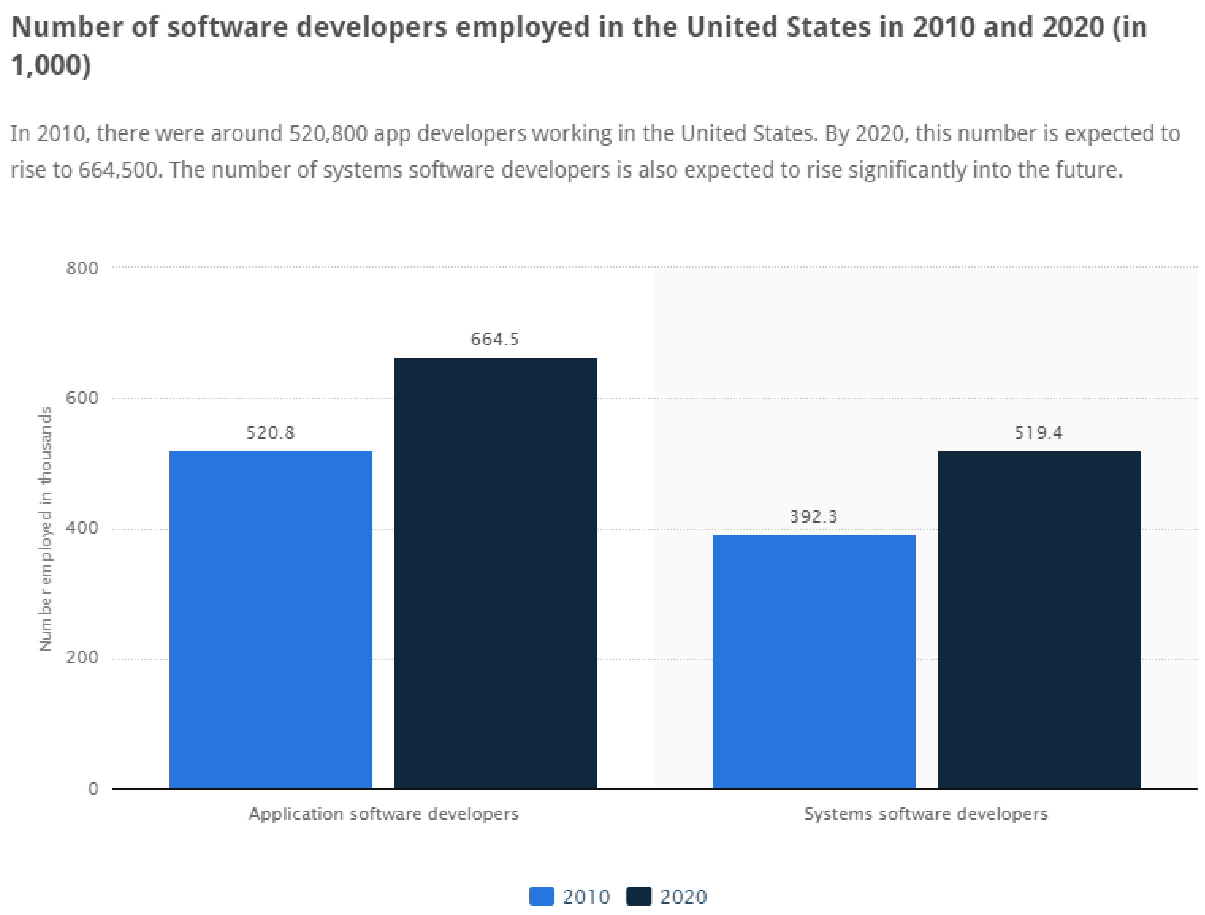
Key highlights of the report include[8]:

- $350 billion market breaks out to $282 billion in private sector spending and $69 billion in federal government spending on homeland security
- Operational (non-IT) private security spending is estimated to be $202 billion with expected growth of 5.5 percent in 2013; IT-related private security market is estimated at $80 billion with growth of 9 percent projected for 2013
- Number of full-time security workers is estimated to be between 1.9 and 2.1 million
- 42 percent of respondents indicated spending on training would increase in 2013, with 12 percent anticipating a rise of 10 percent or more

[8] https://www.asisonline.org/News/Press-Room/Press-Releases/2013/Pages/Groundbreaking-Study-Finds-U.S.-Security-Industry-to-be-$350-Billion-Market.aspx

- Private detective/investigator is one of the fastest growing occupations, with anticipated growth of 21 percent projected through 2020; several IT positions are anticipated to grow 22 percent through 2020

Other US stats



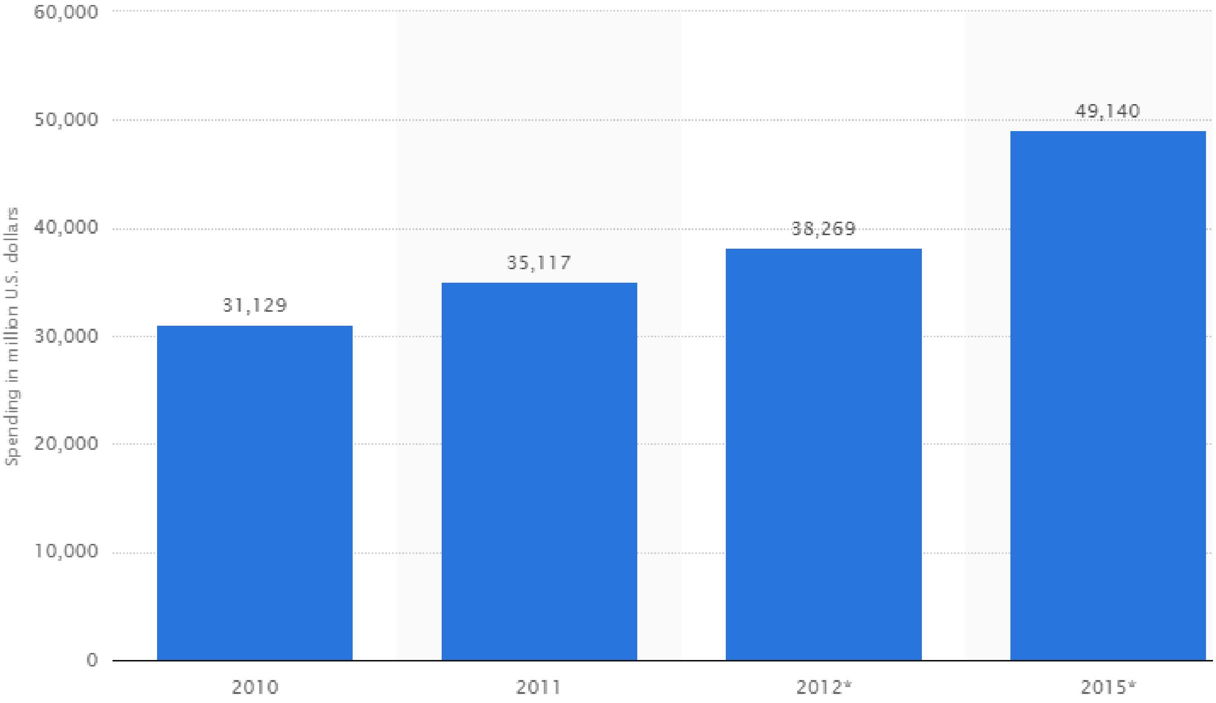
Number of software developers employed in the United States in 2010 and 2020 (in 1,000)

In 2010, there were around 520,800 app developers working in the United States. By 2020, this number is expected to rise to 664,500. The number of systems software developers is also expected to rise significantly into the future.

Source: http://www.statista.com/

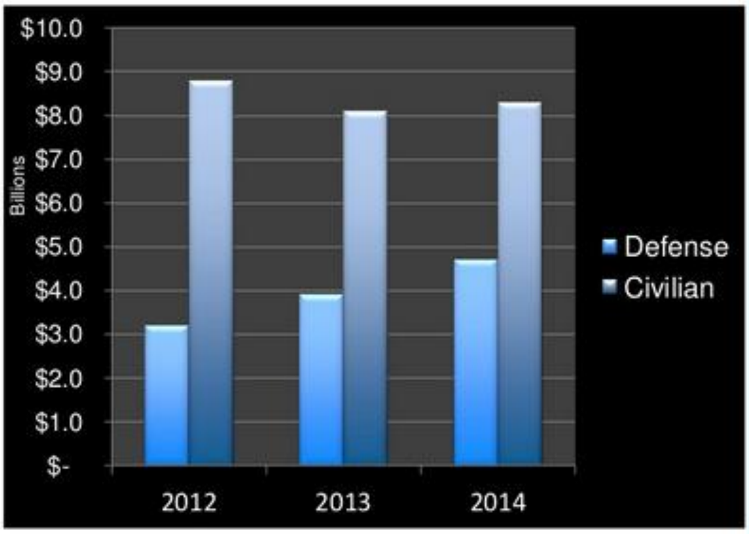
In 2010, there were around 520,800 app developers working in the United States. By 2020, this number is expected to rise to 664,500. The number of systems software developers is also expected to rise significantly into the future.

Job increase rate for information security analysts, web developers, and computer network architects in the United States from 2010 to 2020



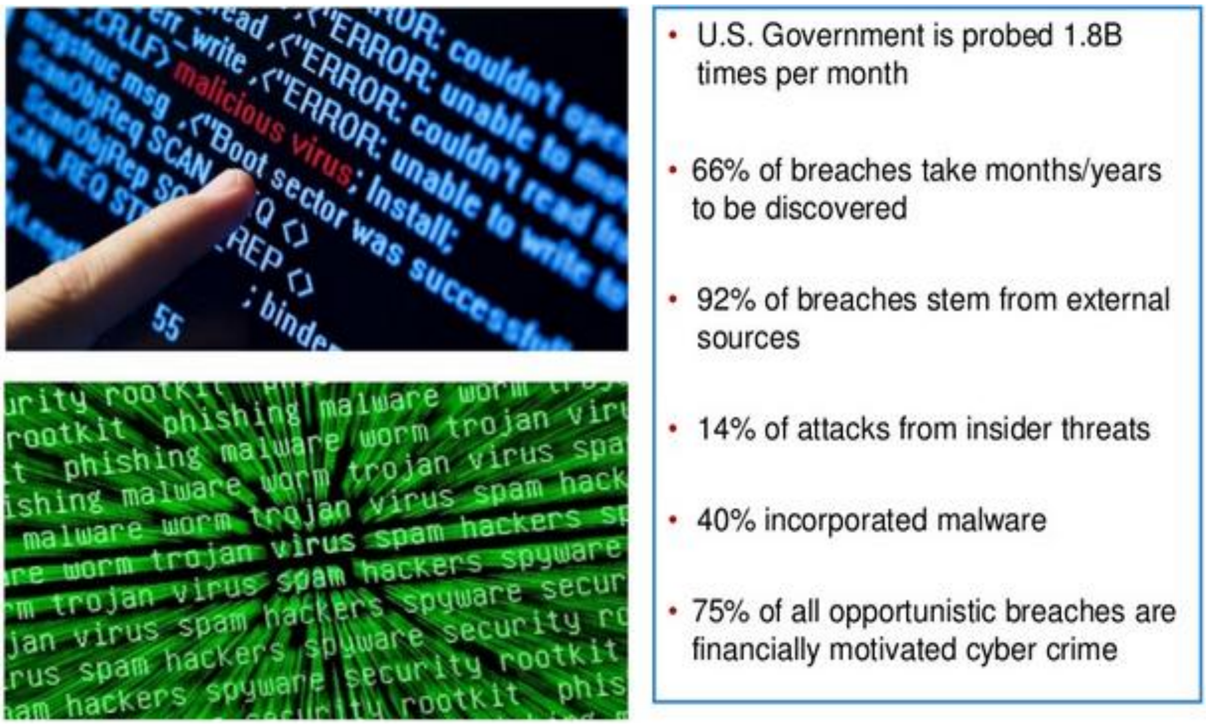
Source: http://www.statista.com/

Here you can see a projection for the employment change from 2010 to 2010 for jobs as information security analysts, web developers, and computer network architects. The source estimates that there will be a 22 percent increase in employment in these areas.

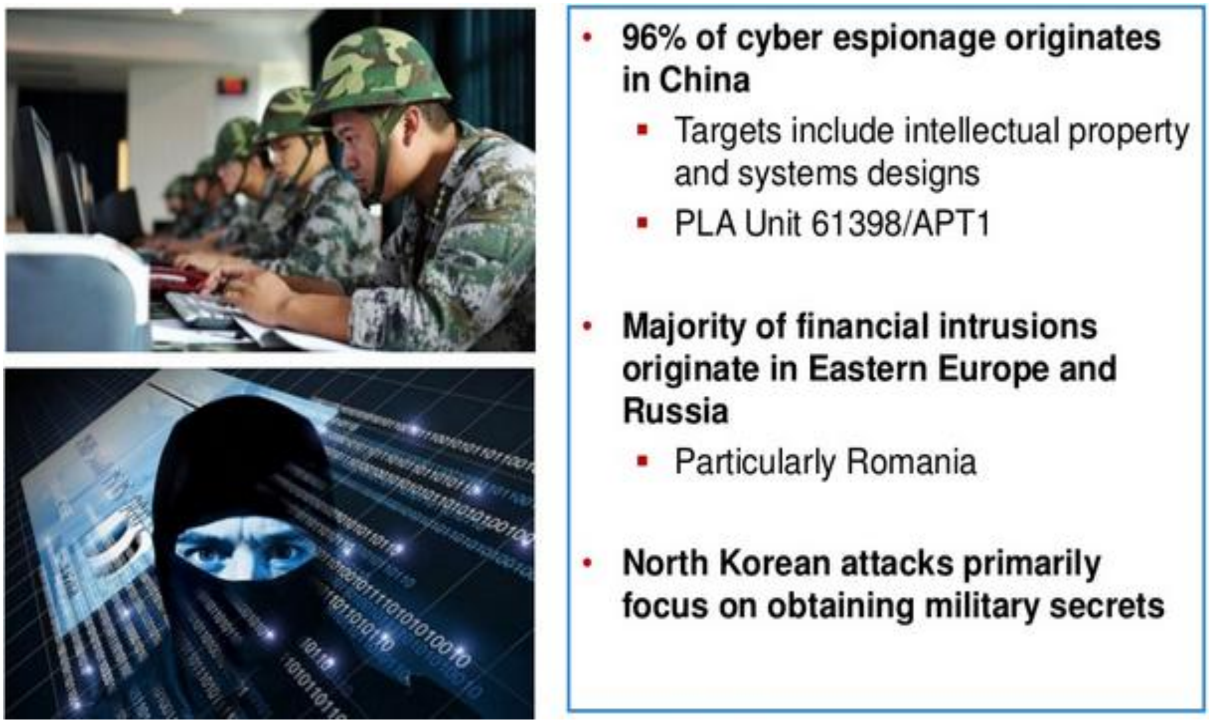


- Improved monitoring and alert technologies
- National Critical Infrastructure Centers
- New funding to expand the Comprehensive National Cyber Security Initiative
- Increased manning of U.S. Cyber Command
- Increased funding for intra-government information sharing

Source: http://www.slideshare.net/immixGroup/cyber-security-slide-deck



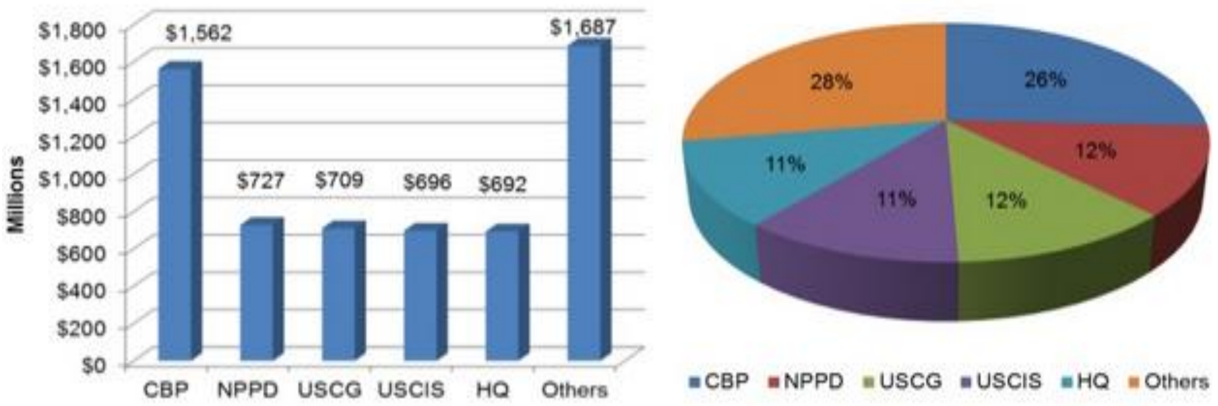
- U.S. Government is probed 1.8B times per month
- 66% of breaches take months/years to be discovered
- 92% of breaches stem from external sources
- 14% of attacks from insider threats
- 40% incorporated malware
- 75% of all opportunistic breaches are financially motivated cyber crime

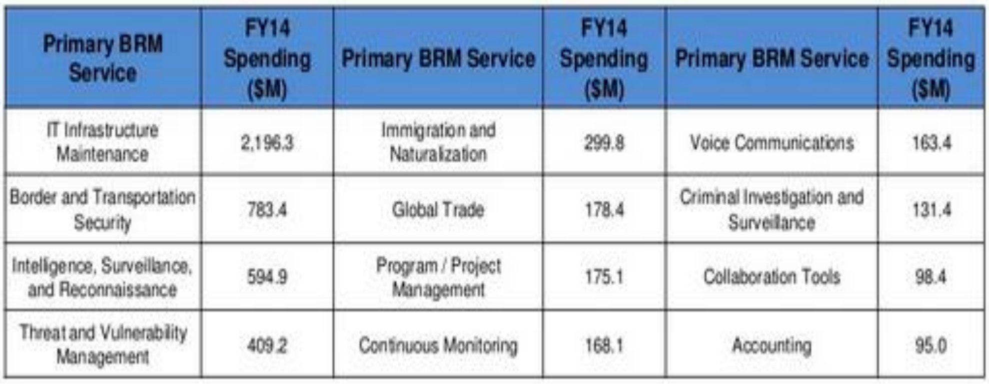


- **96% of cyber espionage originates in China**
  - Targets include intellectual property and systems designs
  - PLA Unit 61398/APT1
- **Majority of financial intrusions originate in Eastern Europe and Russia**
  - Particularly Romania
- **North Korean attacks primarily focus on obtaining military secrets**

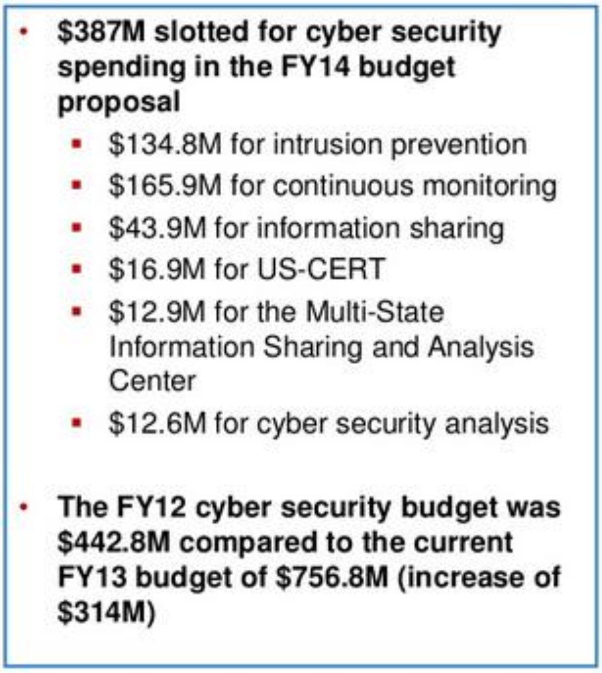
Source: http://www.slideshare.net/immixGroup/cyber-security-slide-deck

Total DHS FY14 IT Budget: $6.1B





Primary BRM Service	FY14 Spending ($M)	Primary BRM Service	FY14 Spending ($M)	Primary BRM Service	FY14 Spending ($M)
IT Infrastructure Maintenance	2,196.3	Immigration and Naturalization	299.8	Voice Communications	163.4
Border and Transportation Security	783.4	Global Trade	178.4	Criminal Investigation and Surveillance	131.4
Intelligence, Surveillance, and Reconnaissance	594.9	Program / Project Management	175.1	Collaboration Tools	98.4
Threat and Vulnerability Management	409.2	Continuous Monitoring	168.1	Accounting	95.0

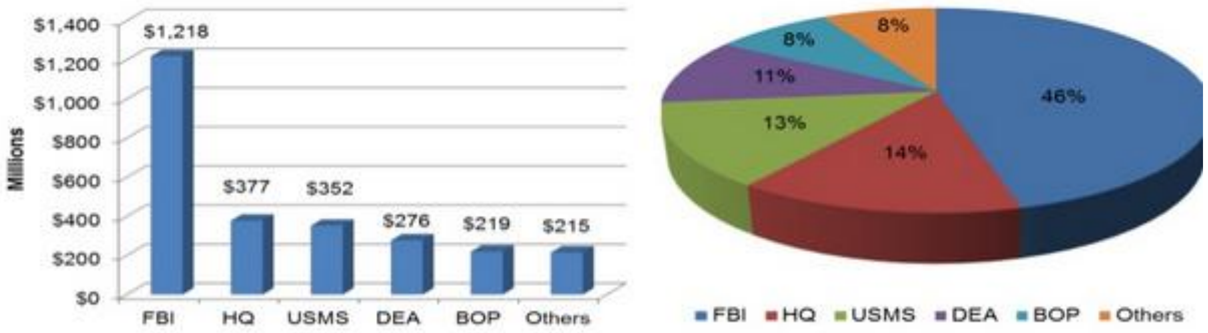


- **$387M slotted for cyber security spending in the FY14 budget proposal**
  - $134.8M for intrusion prevention
  - $165.9M for continuous monitoring
  - $43.9M for information sharing
  - $16.9M for US-CERT
  - $12.9M for the Multi-State Information Sharing and Analysis Center
  - $12.6M for cyber security analysis
- **The FY12 cyber security budget was $442.8M compared to the current FY13 budget of $756.8M (increase of $314M)**

Source: http://www.slideshare.net/immixGroup/cyber-security-slide-deck

Department of Justice IT Spend

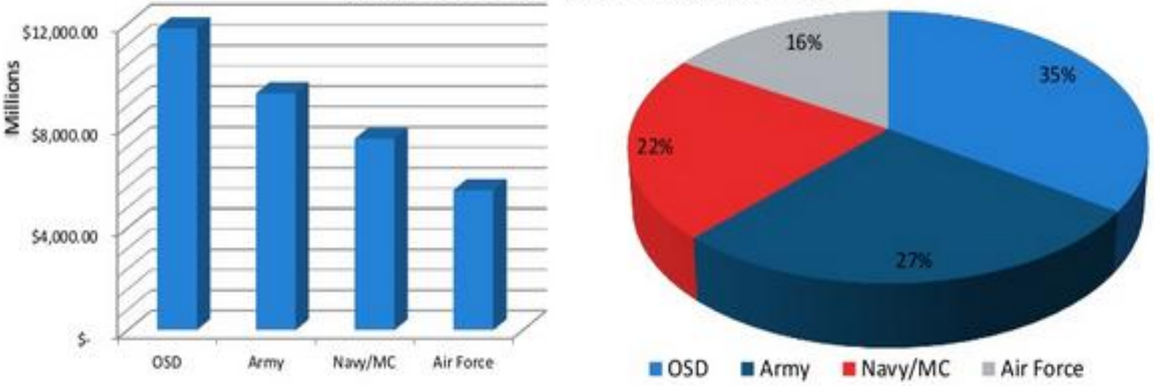
Total DOJ FY14 IT Budget: $2.7B



Primary BRM Service	FY13 Spending ($M)	Primary BRM Service	FY13 Spending ($M)	Primary BRM Service	FY13 Spending ($M)
IT Infrastructure Maintenance	641.5	Threat and Vulnerability Management	130.8	Legal Prosecution and Litigation	52.6
Criminal Investigation and Surveillance	557.9	Accounting	125.1	IT Strategy and Innovation	50.2
Computer/ Network Integration	223.8	Criminal Incarceration	112.2	Crime Prevention	42.4
Criminal and Terrorist Threat Mitigation	201.4	Intelligence, Surveillance, and Reconnaissance	99.4	Voice Communications	41.8

Department of Defense IT Spending

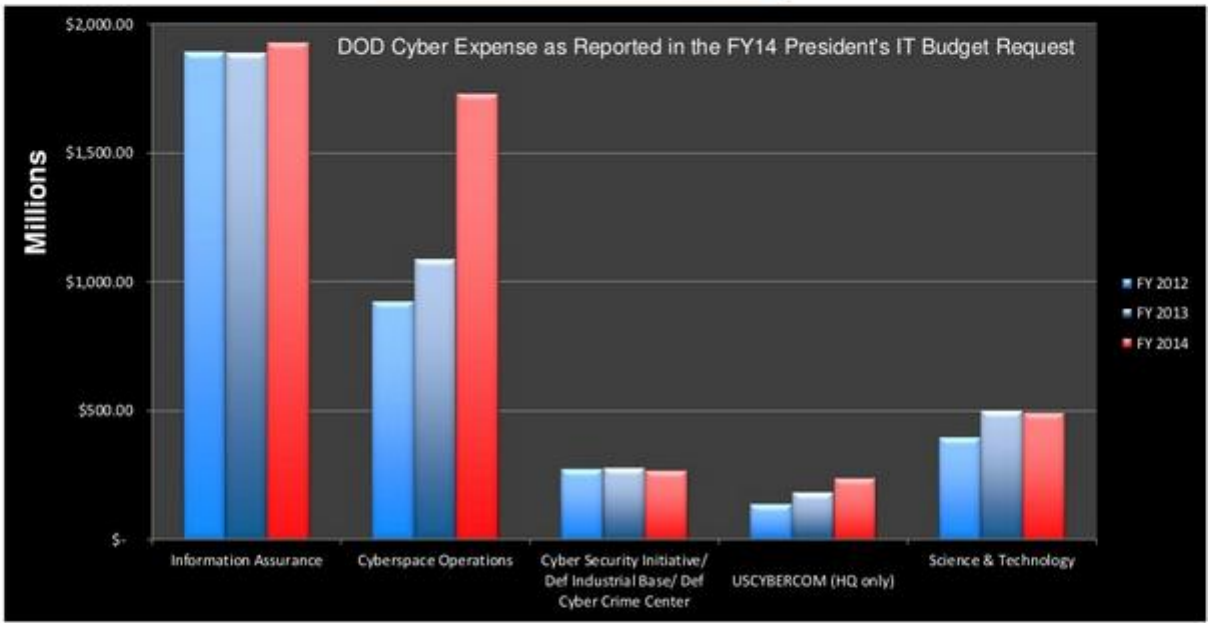
Total DOD FY14 IT Budget: $39.9B



Primary BRM Service	Total FY2013 Spending ($M)	Primary BRM Service	Total FY2013 Spending ($M)
IT Infrastructure Maintenance	13,749.4	IT System Development / Integration Support	92.3
Battlespace Networks	4,217.8	Enterprise Architecture	50.4
Command and Control	2,292.9	Intelligence, Surveillance, and Reconnaissance	41.0
Computer/ Network Integration	370.0	Payroll	36.7

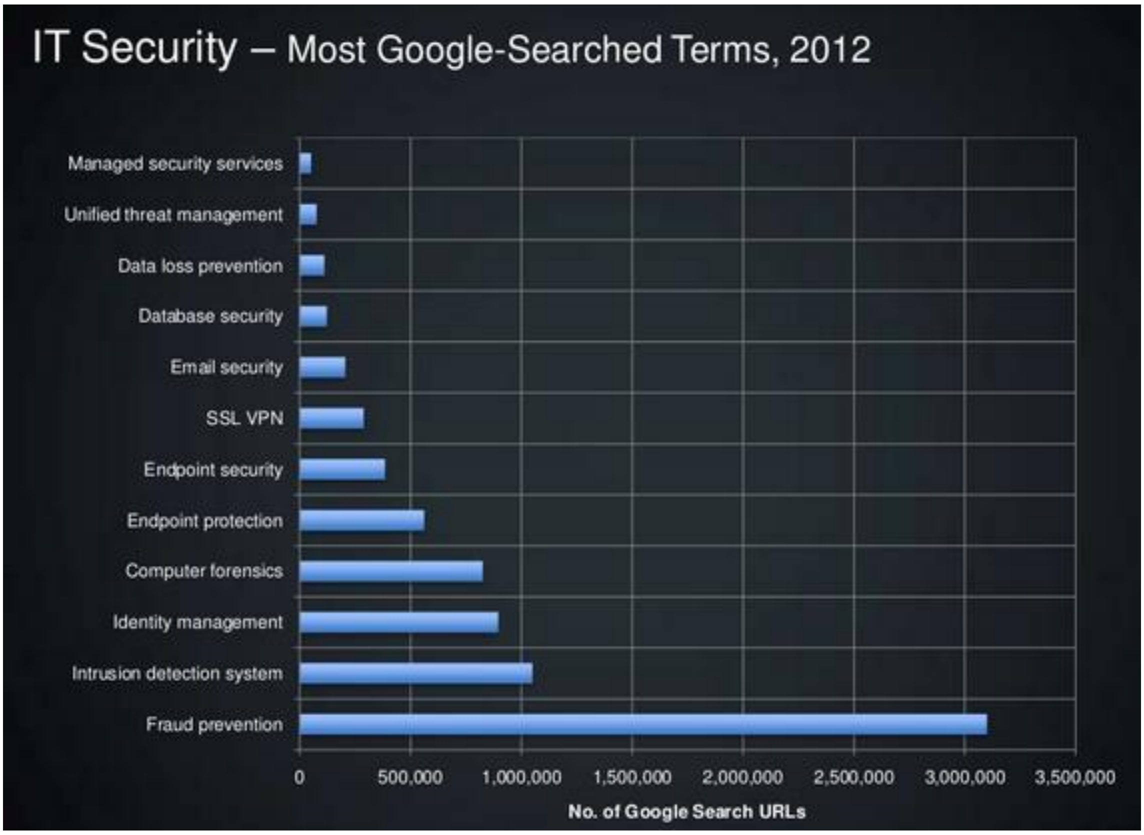
Source: http://www.slideshare.net/immixGroup/cyber-security-slide-deck

DOD Cyber Budget



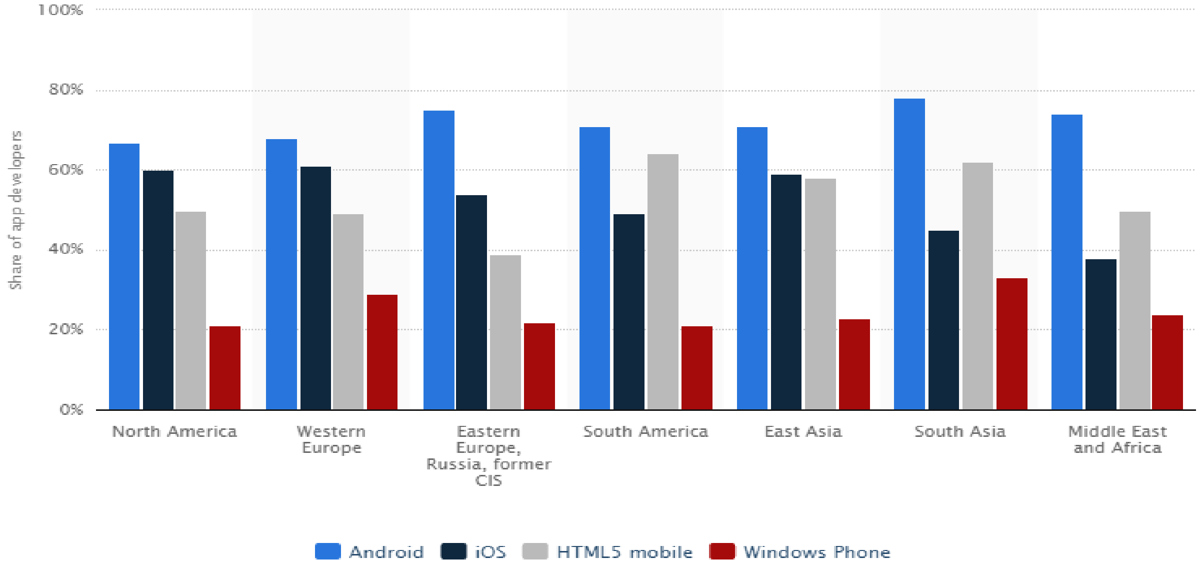
Source: http://www.slideshare.net/immixGroup/cyber-security-slide-deck

Other World



Source: http://www.slideshare.net/

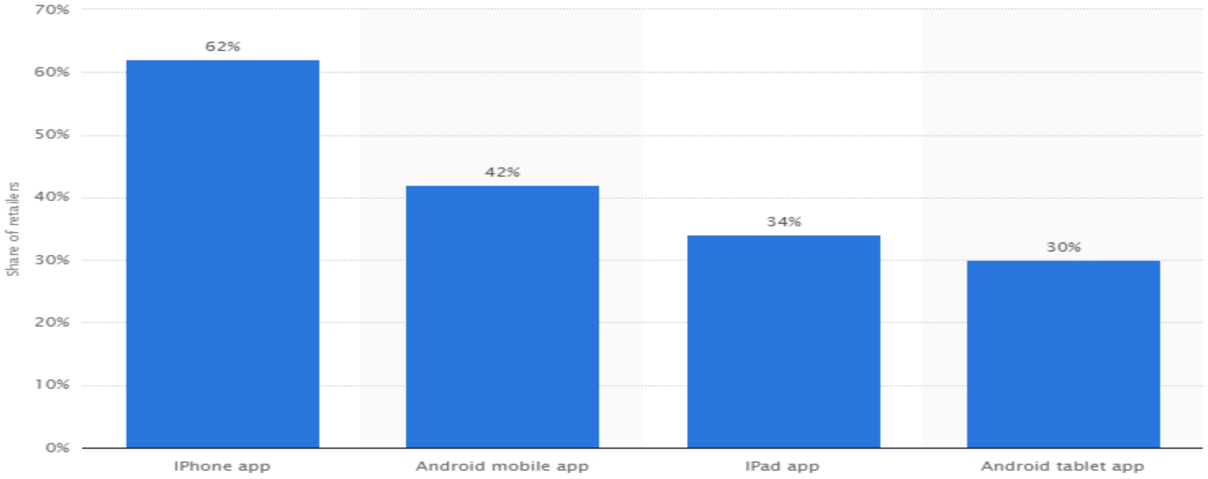
Selected mobile platforms used by app developers worldwide as of 1st quarter 2014, by region



Source: http://www.statista.com/

This statistic shows a mobile platforms used by app developers worldwide, sorted by region. As of the first quarter of 2014, 67 percent of app developers in North America used the Android platform. In South Asia, the share of programmers developing on the Android system was 78 percent.

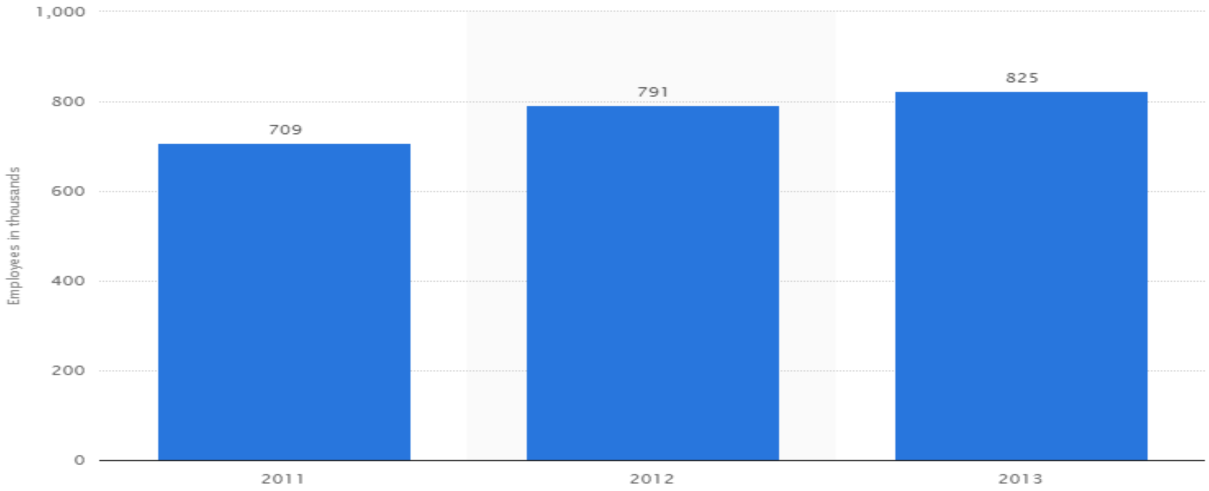
Share of retailers offering mobile apps in the United Kingdom (UK) as of July 2013, by device and OS



Source: http://www.statista.com/

This statistic displays the share of retailers offering mobile apps in the United Kingdom (UK) by device and OS. Of retailers, 42 percent offered an Android phone app, while 30 percent offered an Android tablet app.

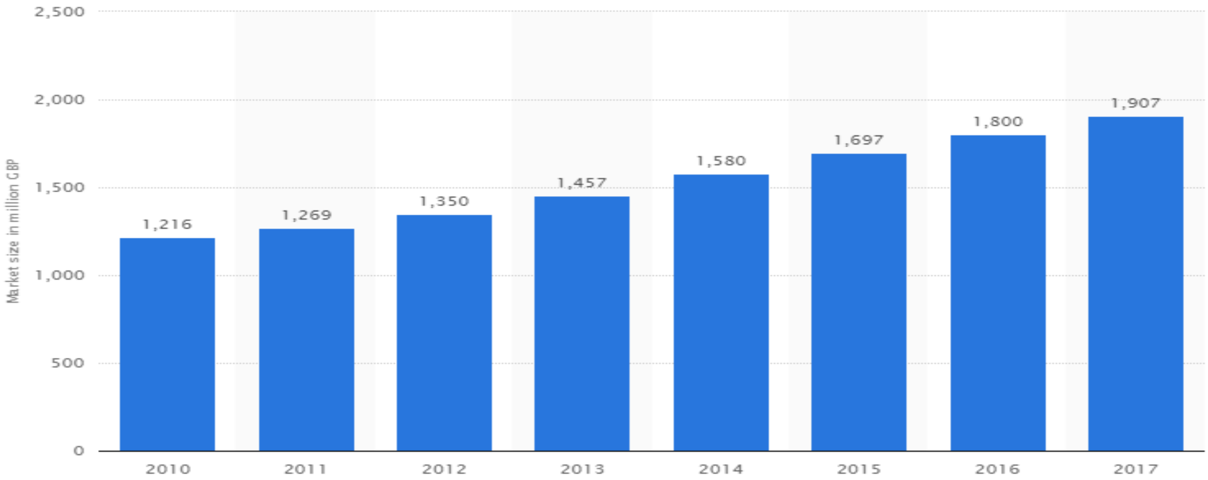
Number of employees in the IT, software and computer services economy of United Kingdom (UK) from 2011 to 2013* (in 1,000s)



Source: http://www.statista.com/

This statistic displays IT, software and computer services economy employment in the United Kingdom (UK) from 2011 to 2013. In 2011, 709 thousand people were employed in jobs in this economy--a figure that includes employment at companies and organizations not directly classified within these industries, including: IT and telecommunications directors, IT business analysts, architects and systems designers, programmers and software development professionals, web design and development professionals.

Total cyber security market size of the software & IT services segment in the United Kingdom (UK) from 2010 to 2017 (in million GBP)

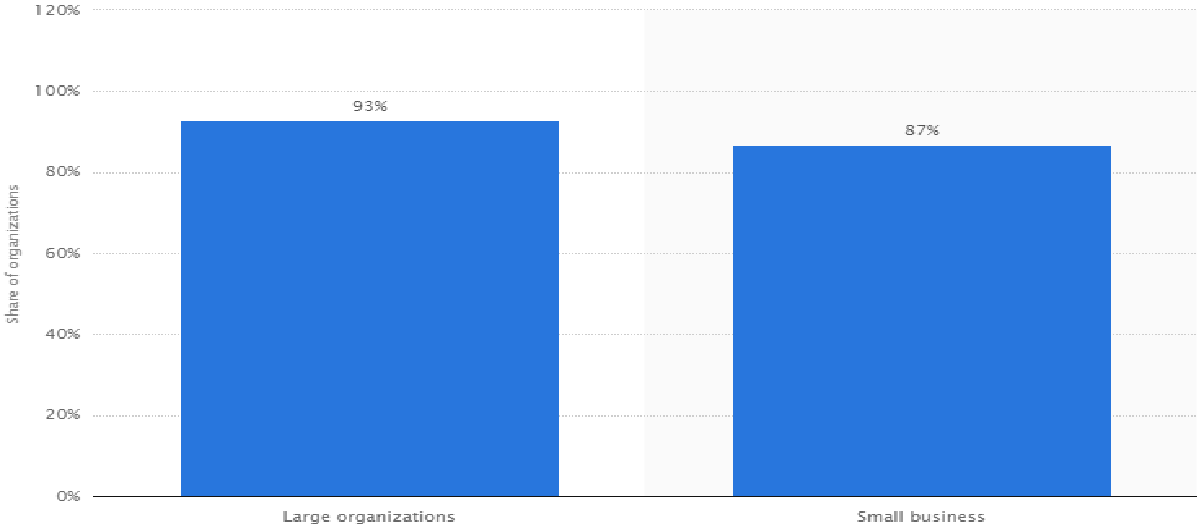


Source: http://www.statista.com/

This statistic shows the market size forecast of the total software & IT services segment, which includes the software and project services and outsourcing segments and is part of the cyber security market analysed by IT product and service type, in the United

Kingdom (UK) from 2010 to 2017. The estimated cyber security market size of the total software & IT services segment in 2017 is 1.9 billion British pounds (GBP).

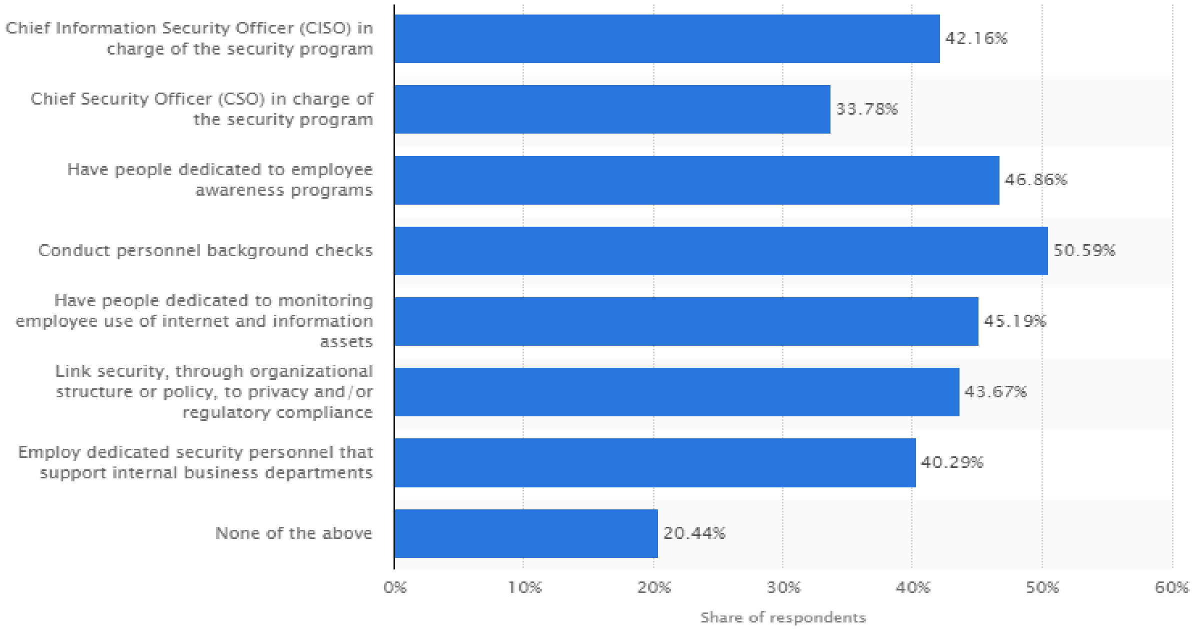
Share of organizations in the United Kingdom that experienced a security breach within the last year as of early 2013, by organization size



Source: http://www.statista.com/

This statistic shows the share of organizations in the United Kingdom, who had experienced a security breach in the past year as of February/March 2013. This was more common in larger organizations, 93 percent of larger organizations reported a breach of some kind.

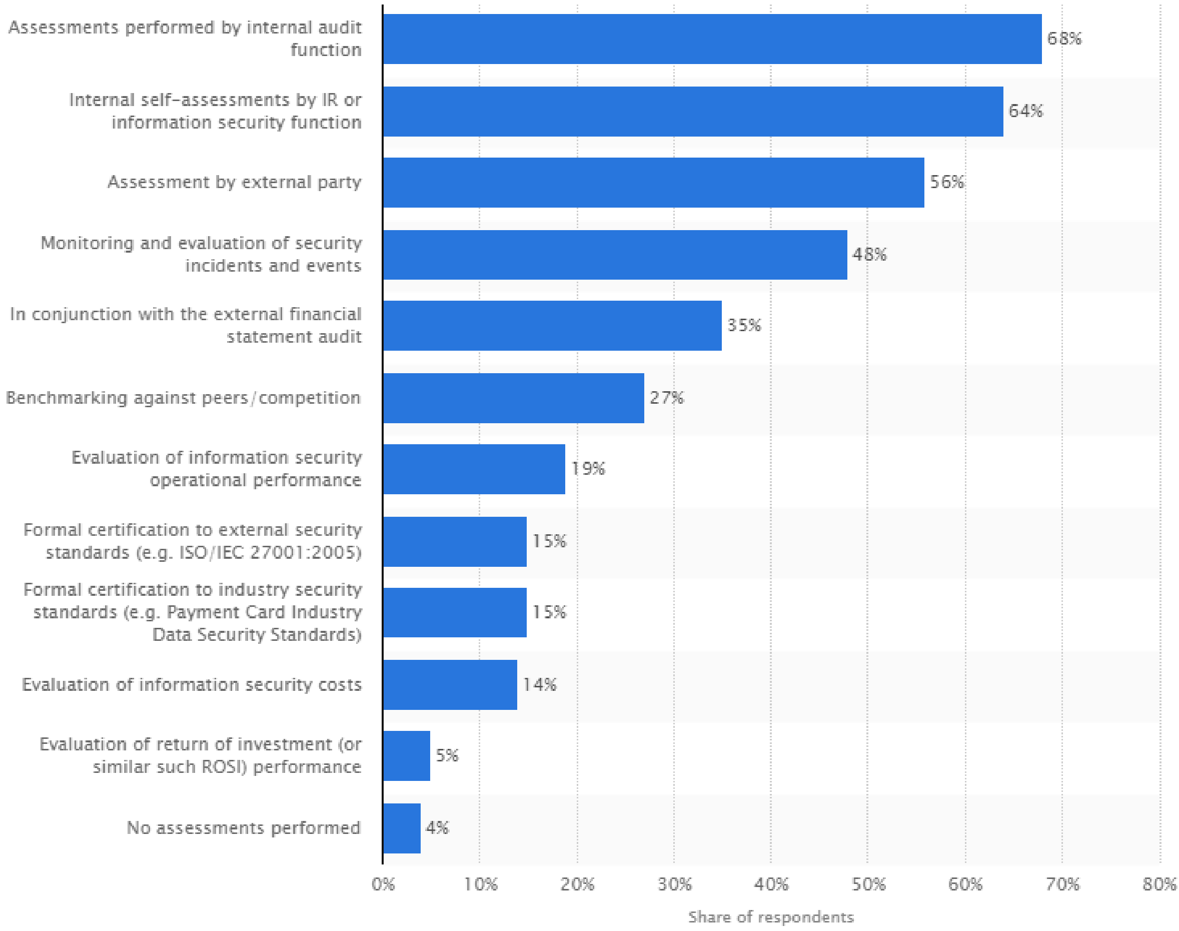
What information security safeguards related to people does your organization currently have in place?



Source: http://www.statista.com/

In 2012, PwC conducted a survey of businesses around the world, asking what kinds of information security safeguards related to people their company had in place at that time. 42.16 percent of organizations reported that they had a CISO manager in charge of security programs.

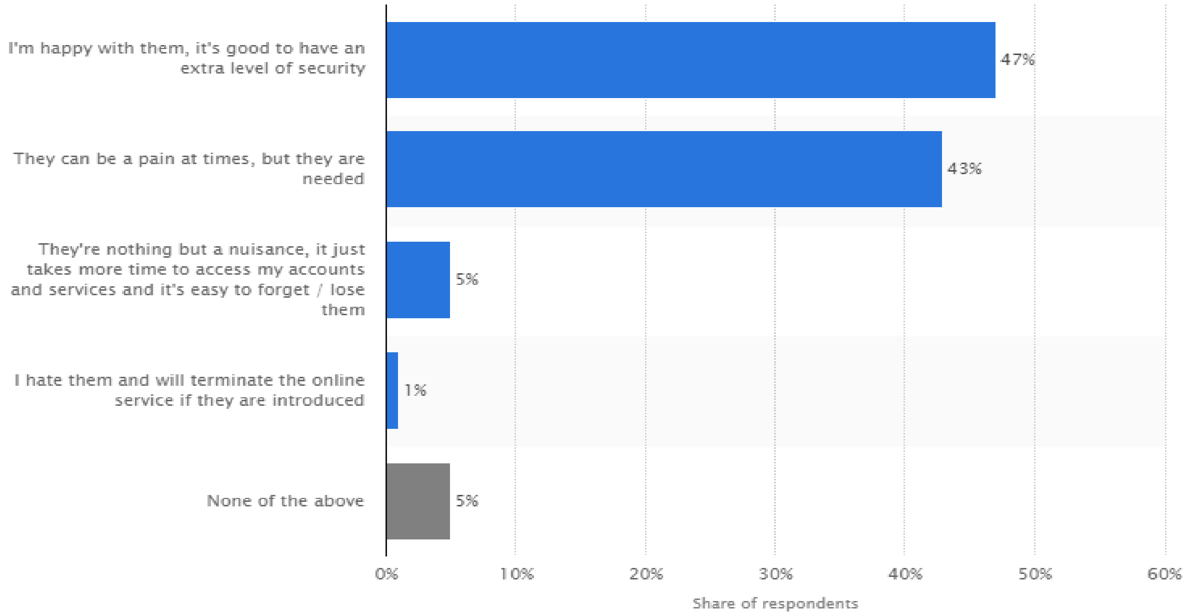
How does your organization assess the efficiency and effectiveness of information security?



Source: http://www.statista.com/

Through a survey conducted in the middle of 2012 it was found that 68 percent of organizations assessed the efficiency and effectiveness of their information security functions through assessments performed by internal audit functions.

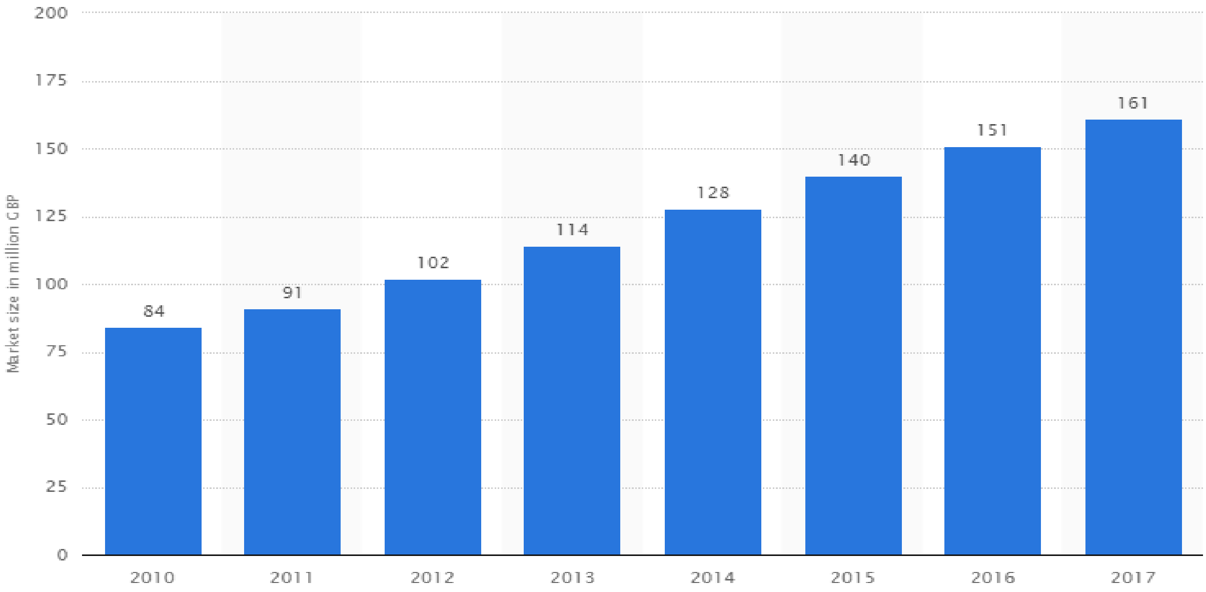
Which statement best describes your opinion of additional security layers used by online services (e.g. online banking services)?*



Source: http://www.statista.com/

This statistic displays the opinions of British survey respondents of additional or supplementary security layers (e.g. additional passwords sent by SMS, additional security questions, etc.) used by online services. As of November to December 2013, 47 percent of British respondents reported being happy to have extra security.

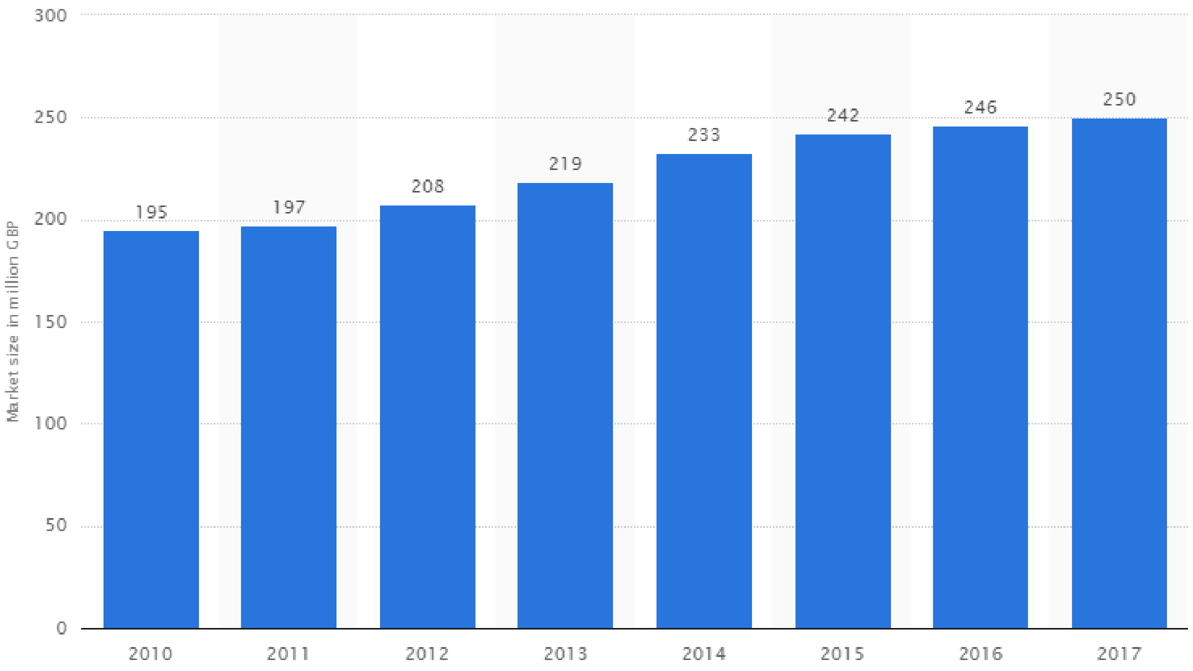
Cyber security market size of the management consultancy segment in the United Kingdom (UK) from 2010 to 2017 (in million GBP)



Source: http://www.statista.com/

This statistic shows the market size forecast of the management consultancy segment, which is part of the cyber security market analysed by IT product and service type, in the United Kingdom (UK) from 2010 to 2017. The estimated cyber security market size of the management consultancy segment in 2017 is 161 million British pounds (GBP).

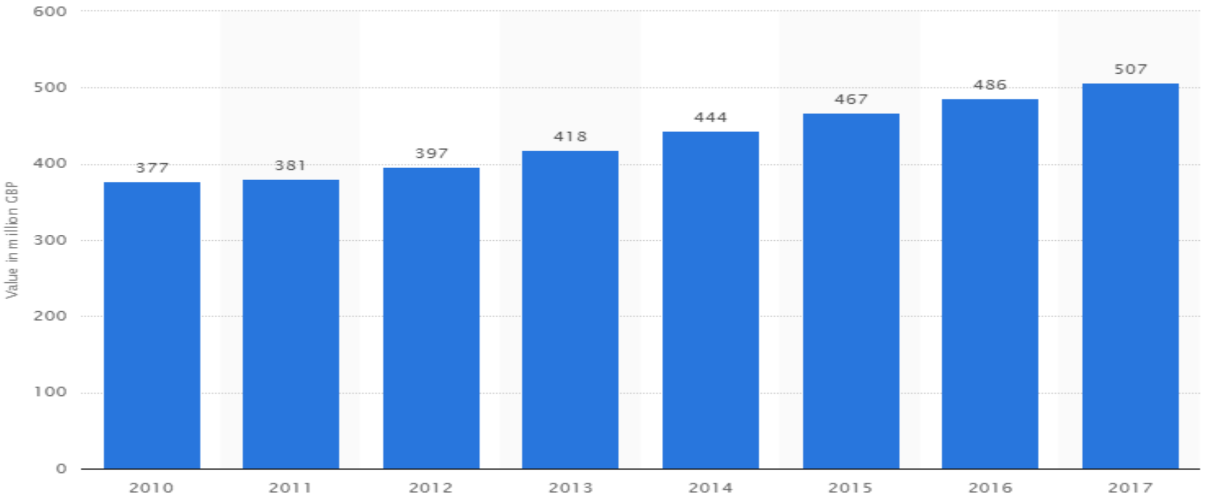
Cyber security market size of defence and intelligence in the United Kingdom (UK) from 2010 to 2017 (in million GBP)



Source: http://www.statista.com/

This statistic shows the market forecast for the cyber security defence and intelligence segment in the United Kingdom (UK) from 2010 to 2017. The estimated size of the defence and security subsector in 2017 was 250 million British pounds (GBP).

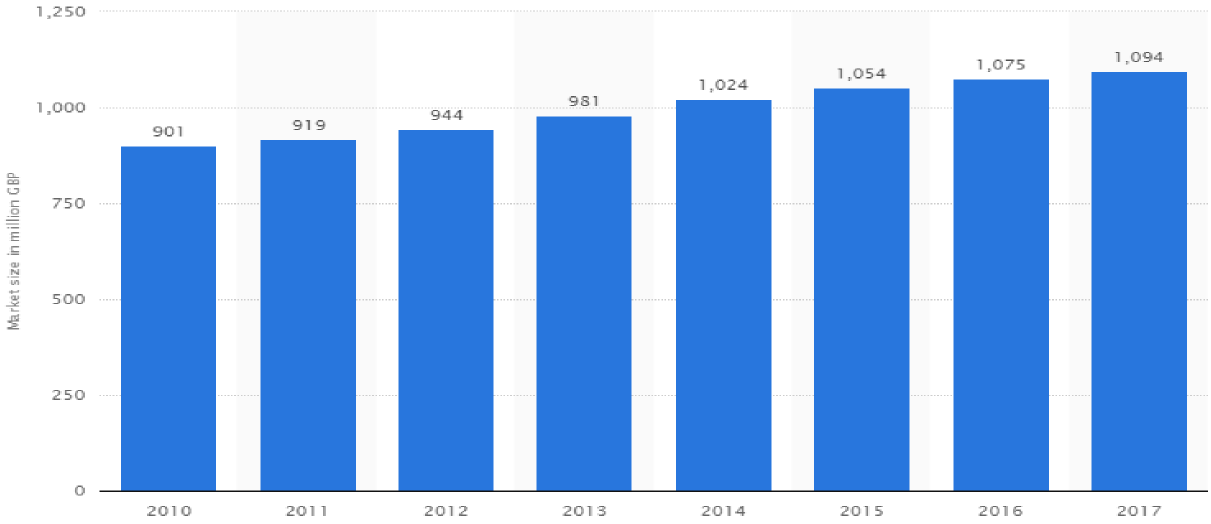
Cyber security market size of network equipment in the United Kingdom (UK) from 2010 to 2017 (in million GBP)



Source: http://www.statista.com/

This statistic shows the market size forecast of the network equipment segment, which is part of the cyber security market analysed by IT product and service type, in the United Kingdom (UK) from 2010 to 2017. The estimated cyber security market size of the network equipment segment in 2017 is 507 million British pounds (GBP).

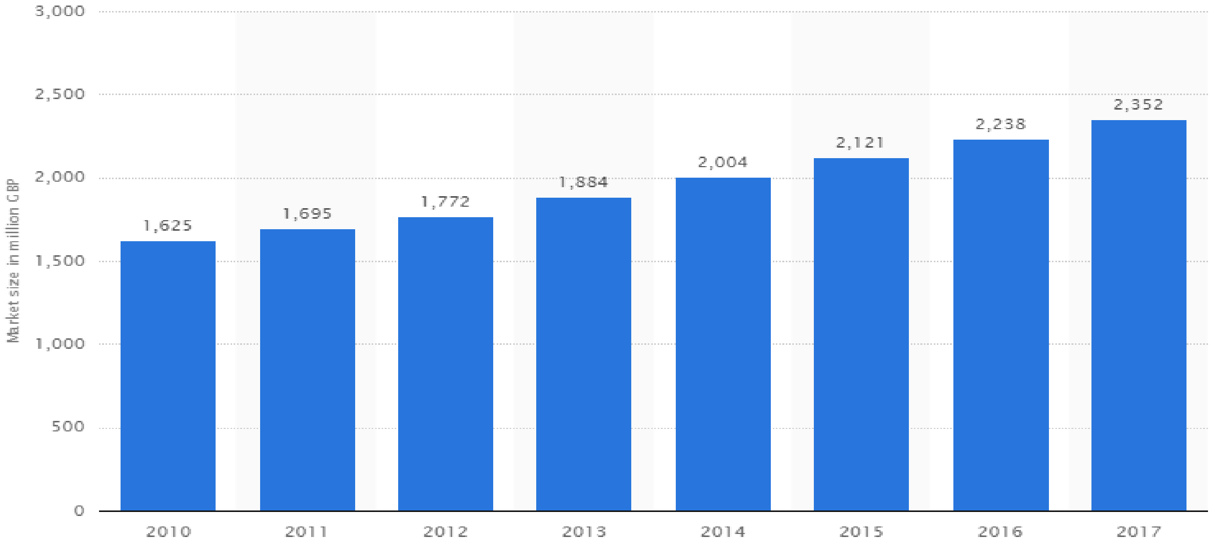
Cyber security market size of the infrastructure solutions segment in the United Kingdom (UK) from 2010 to 2017 (in million GBP)



Source: http://www.statista.com/

This statistic show the market size forecast of the infrastructure solutions segment, which is a part of the cyber security segment, in the United Kingdom (UK) from 2010 to 2017. The estimated cyber security market size of the segment in 2017 is 1,094 million British pounds (GBP).

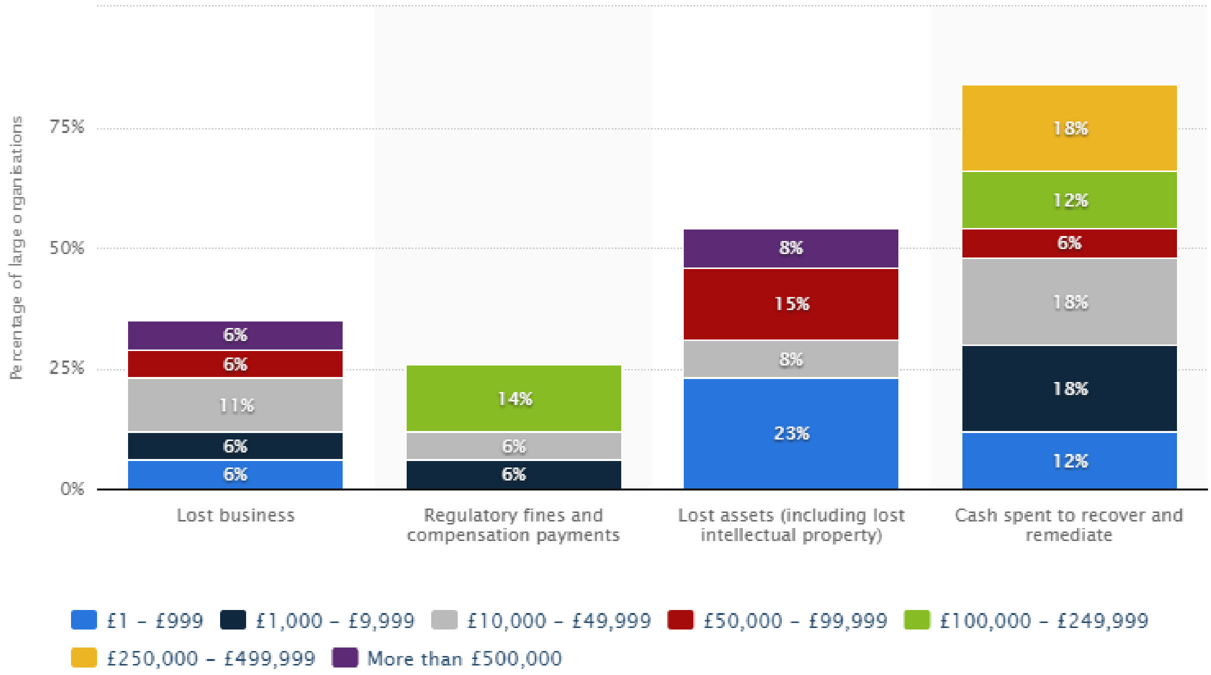
Cyber security market size of the private sector in the United Kingdom (UK) from 2010 to 2017 (in million GBP)



Source: http://www.statista.com/

This statistic shows the market forecast of the total private cyber security sector in the United Kingdom (UK) from 2010 to 2017. The estimated cyber security market size of the private sector in 2017 is 2,352 million British pounds (GBP).

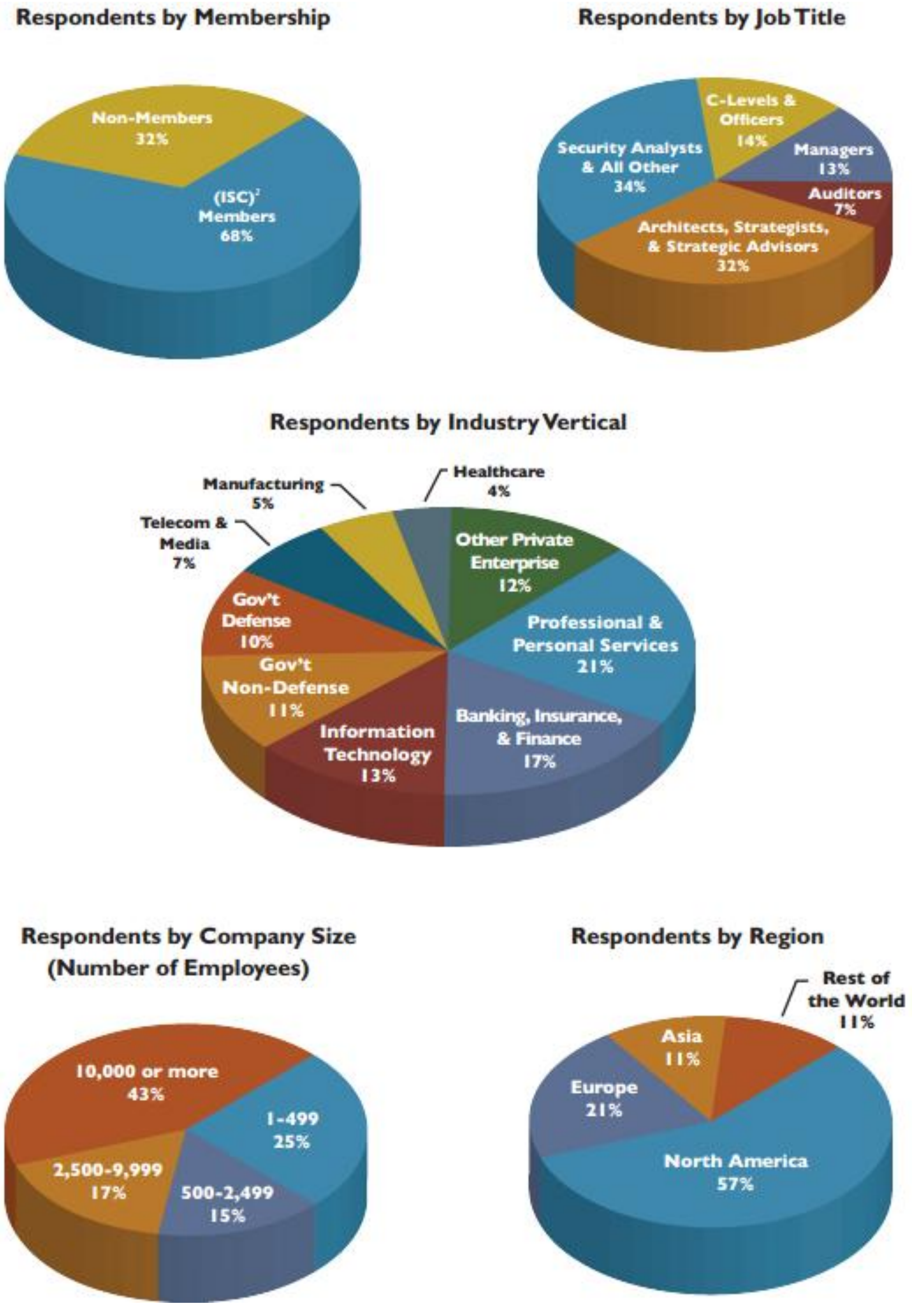
Distribution of large organisations by spending on their worst IT security incident in the United Kingdom (UK) in 2014



Source: http://www.statista.com

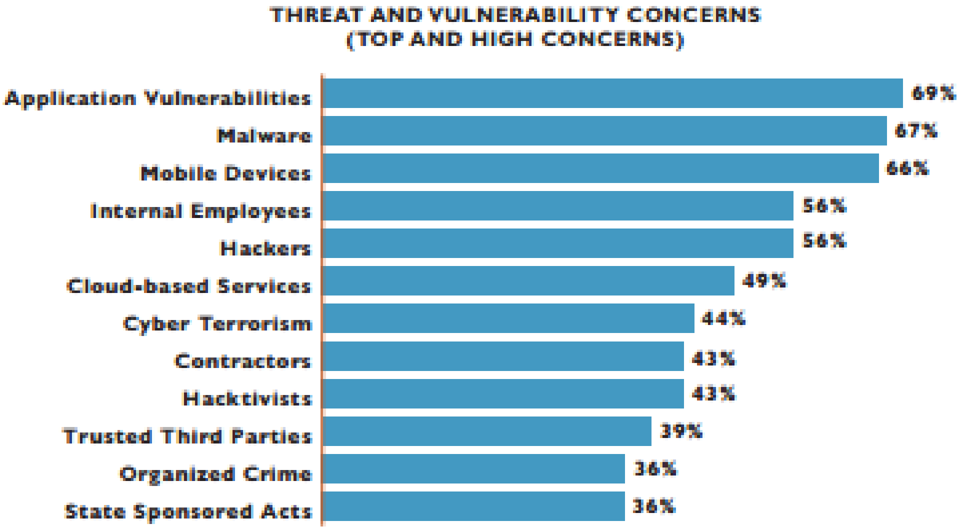
This statistic shows distribution of large organisations by spending on their worst security incident in the United Kingdom (UK) in 2014. From the respondents, 8 percent reported losses of more than 500,000 GBP related to loss of assets.

GISWS Survey



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

As reported in previous GISWS surveys, there is no lack of diversity in the threats and vulnerabilities information security professionals are tackling—and concerned about. All of the 12 threats and vulnerabilities presented in the survey were selected as top or high concerns for 36 percent or more of the survey respondents. At the top of the list, application vulnerabilities, malware, and mobile devices were each identified as a top or high concern by two-thirds or more of the respondents.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Greater examination of Bring Your Own Device (BYOD), including mobile devices, cloud computing, and social media, and their security implications and how information security professionals are responding, is included later in this paper. Secure software development, the upfront means to lessen application vulnerabilities, will also be examined later in this paper. Focusing deeper into the responses on threats and vulnerabilities reveals that concern severity varies.

Some perspectives change over time – Comparing this year’s survey to the 2011 results, the level of concern is fairly stable. However, there was a notable increase in cloud-based services. Compared to the 49 percent of respondents that view cloud-based services as either a top or high security concern in the 2013 survey, 43 percent viewed it as a top or high security concern in the 2011 survey. We believe this increase follows the increased adoption of cloud-based services over the two-year period since the last survey, combined with the resilient security concerns, real and perceived, associated with cloud-based services.

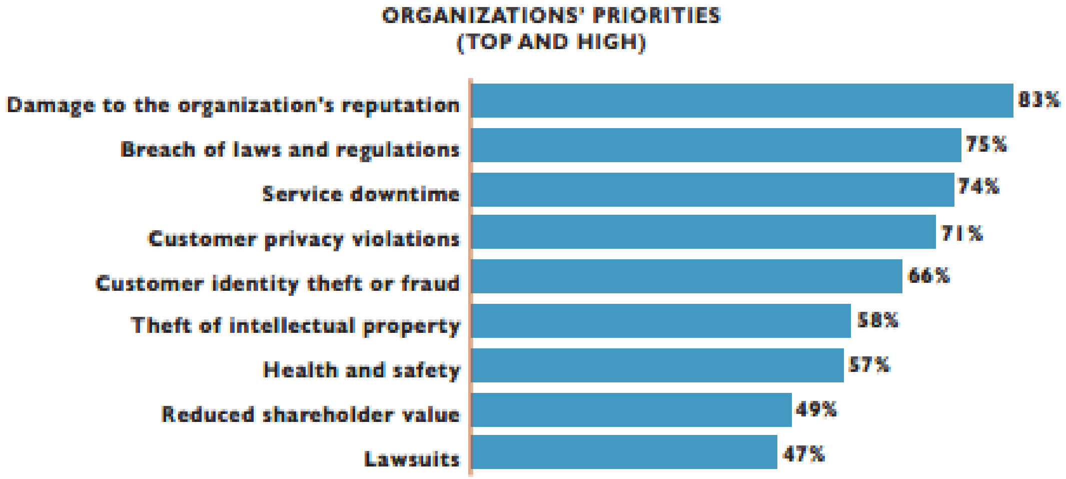
C-levels and officers rated nearly all threat and vulnerability categories higher than respondents in other job titles – This was most notable in application vulnerabilities and mobile device security. Top or high concern was selected by 72 percent of C-levels and officers for application vulnerabilities and 70 percent for mobile devices.

Size and anxiety is correlated – In all threat and vulnerability categories, the average level of concern increased as company size increased. Perhaps the bigger the company is, the more resources it devotes to examining these threats and through that examination, gains a more comprehensive and realistic appreciation of risk and risk implications. Also, from the “greatest gain for the effort mentality,” larger companies represent more lucrative targets for attackers and hackers, thus contributing to a higher level of concern among large company respondents.

Vertical equates to variability – The nature of a company's business and operations also has implications on being a target and with that, variation in concern. No surprise, respondents in the banking, insurance, and finance verticals, with their possession and use of valuable and exploitable personally identifiable and financial information, view the threats posed by hackers, hacktivists, and organized crime higher than the majority of other verticals. Government respondents, also not a surprise, view the threat of state-sponsored acts and cyber terrorism as a greater security concern (i.e., choosing top or high concern) over private enterprises by more than 20 percentage points in each of these threat categories.

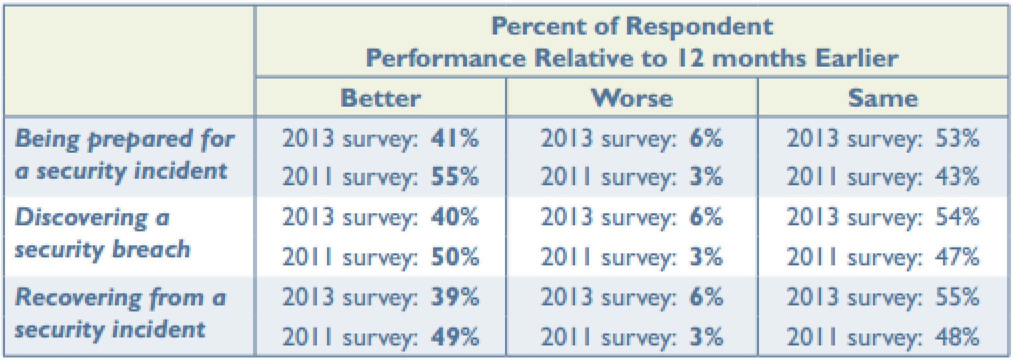
Developing countries express higher level of concern – Survey respondents located in developing countries state a higher level of concern for a majority of the threat and vulnerability categories versus respondents in developed countries. Directly contributing to this is that information security investments in developing countries are historically less than the global average. This is reflected in the lower level of security certifications in developing versus developed countries. For example, with the most popular certification chosen by survey respondents—Certified Information Systems Security Professional (CISSP®)—only 42 percent of the survey respondents located in developing countries (members and non-members combined) had acquired and maintained this certification, versus 71 percent of respondents located in developed countries.

Threats and vulnerabilities have implications—attackers are successful and vulnerabilities are exploited. To that point, the survey asked respondents to rank their organizations' priorities: In other words, what needs to be avoided? As shown, damage to the organization's reputation, breach of laws and regulations, and service downtime represent the top three to-be-avoided outcomes. Also noteworthy is the high percentage of top-priority selections. For example, 49 percent of all survey respondents rated damage to the organization's reputation as a top priority. In fact, five of the nine categories received a top-priority rating by more than one-third of the survey respondents. Conclusion: the "protect and secure" activities of information security professionals are strongly aligned with many high priorities of their organizations.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

With a diversity of threats and vulnerabilities to be concerned with and the need to avoid a range of undesirable outcomes, it is logical to ask about preparedness. In a repeat of the 2011 survey, the 2013 survey requested the respondents judge their change in readiness relative to 12 months earlier (perform better, worse, or same). The results for both surveys are summarized in the following table.

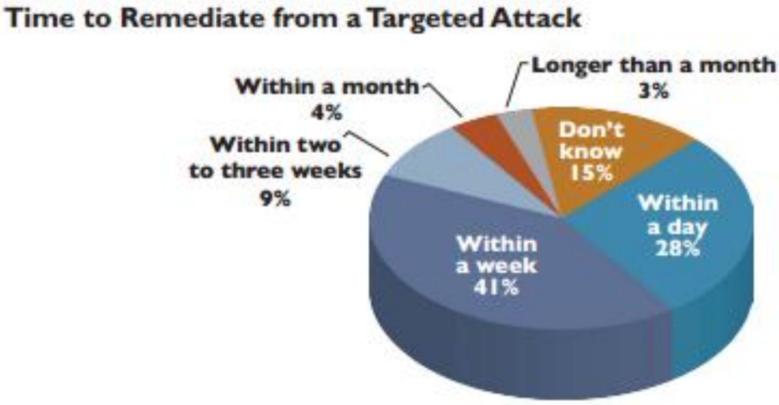


	Percent of Respondent Performance Relative to 12 months Earlier		
	Better	Worse	Same
Being prepared for a security incident	2013 survey: **41%** 2011 survey: **55%**	2013 survey: **6%** 2011 survey: **3%**	2013 survey: 53% 2011 survey: 43%
Discovering a security breach	2013 survey: **40%** 2011 survey: **50%**	2013 survey: **6%** 2011 survey: **3%**	2013 survey: 54% 2011 survey: 47%
Recovering from a security incident	2013 survey: **39%** 2011 survey: **49%**	2013 survey: **6%** 2011 survey: **3%**	2013 survey: 55% 2011 survey: 48%

Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

While the majority of respondents believe that their organizations would perform better or the same relative to 12 months earlier, there was a 10-point or more decline in the percent of respondents believing they would perform better in the 2013 survey compared to the 2011 survey. Not as significant, but equally disconcerting about improvement in the state of readiness, twice the percentage of respondents in the 2013 survey view their readiness has worsened in the past year as did respondents in the 2011 survey. As an indication that membership really matters, the survey-over-survey decline in the percent of respondents selecting “better,” and increase in selecting “worse,” was not as profound with member respondents compared to non-member respondents.

Another survey question focused on readiness is how quickly damage from a targeted attack would be remediated. Slightly more than two-thirds of the respondents project that they could remediate the damage from a targeted attack within a week or less. Yet, there is also a material portion of the respondents that are unsure how long damage remediation might take.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

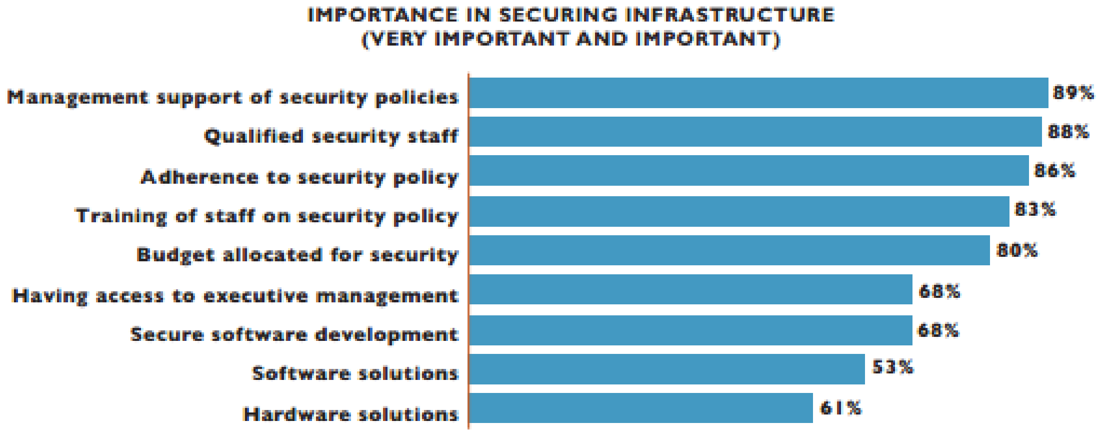
As typical, C-levels voiced greater assurance on their organizations' readiness – C-levels and officers chose "within one day" or "don't know" less than respondents with job titles farther down the organizational structure—31 percent and 10 percent, respectively

Smallness advantage – With a less diverse and smaller spread of operations, 31 percent of small companies (less than 500 employees) believe they can remediate in one day and 44 percent within a week. This is a faster expectation than very large companies (10,000 or more employees)—28 percent and 39 percent, respectively. Also, respondents in very large organizations chose "don't know" to a greater extent (18 percent) than small companies (12 percent).

Experience advantage – Banking, insurance, and finance verticals, plus the info tech vertical, believe they can respond faster than other industries; 34 percent and 32 percent of respondents in those verticals, respectively, predicted within one day to remediate. Potentially due to highly distributed operations, respondents in the retail & wholesale and construction verticals chose "don't know" at higher levels—19 percent and 20 percent, respectively. Potentially, a lack of experience in past remediation efforts influenced 20 percent of respondents in the utilities vertical to choose "don't know.

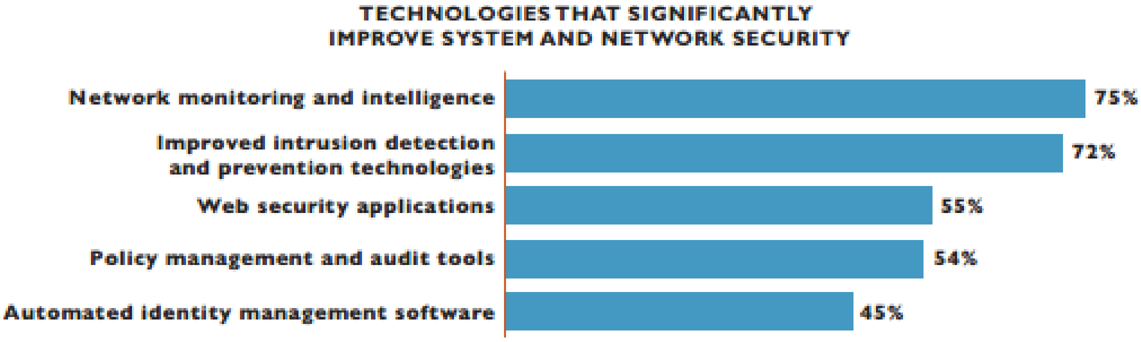
People are a Key Tool in Information Security

With the pervasiveness, diversity, and evolution in security threats, information security professionals use an assortment of tools. Top of the list are human aspects: management support, qualified staff, and policy adherence, with half or greater of respondents choosing very important for each. The next four categories also have a human aspect. Security software and hardware are materially farther down the list of essential tools in effective security; confirming the viewpoint that the effectiveness of security technologies is maximized only when the trained human element is actively incorporated.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Concentrating on select security technologies that provide significant improvement in system and network security (those that garnered more than 10 percent of respondent selection), two technologies were highlighted by the survey respondents for their capabilities: network monitoring & intelligence, and intrusion detection & prevention.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Need and Budget forthe Right Information Security Professional

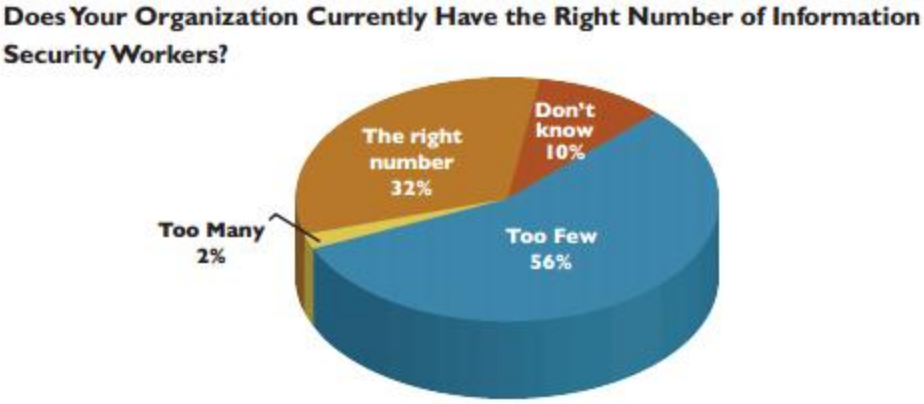
With security staff viewed as critical in importance, it is equally important to understand the acuteness of need, organizations' ability to fund staff expansion and improvement, and the sought-after attributes of information security professionals. The need is present

Very few respondents view their security organizations as being over-staffed. Nearly one-third of respondents believe they have the right number of staff, but more than 50 percent believe staff expansion is justified.

The good news is that two-thirds of C-levels, those with the greatest budgetary influence, view their security organizations as being too few in numbers.

More midsize companies' (500-2,499 employees) respondents view their organizations as understaffed versus smaller and larger size companies.

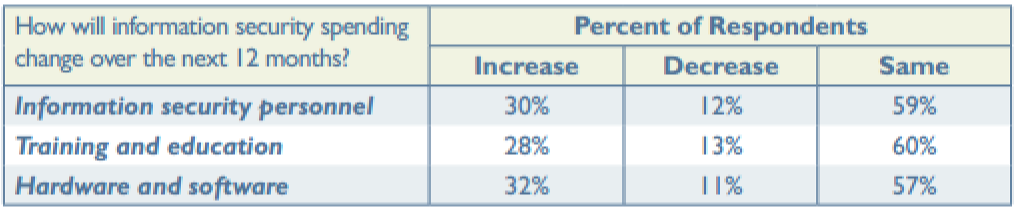
Across industries, a greater percentage of respondents in education, healthcare, manufacturing, and retail & wholesale verticals believe they are understaffed.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Budget availability to increase spending is strong

An increase in spending is predicted by nearly one-third of survey respondents in personnel, training and education, and hardware and software. Slightly more than 10 percent, however, predict a decline. This decline is more prevalent in government (approximately 19 percent of respondents predicting declines) versus private sector (approximately 10 percent of respondents predicting declines). More than any other private sector vertical, 35 percent of respondents in the info tech vertical predict spending increases



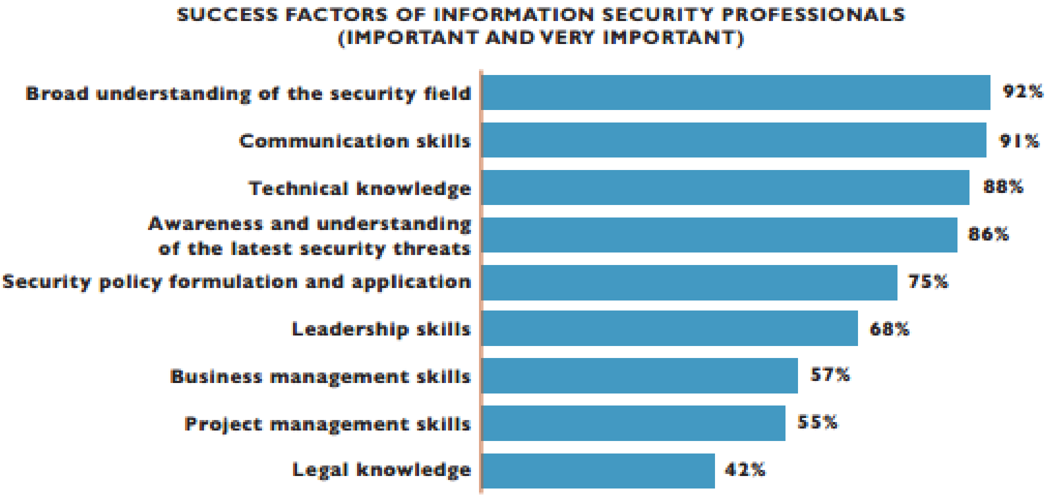
How will information security spending change over the next 12 months?	Percent of Respondents		
	Increase	Decrease	Same
Information security personnel	30%	12%	59%
Training and education	28%	13%	60%
Hardware and software	32%	11%	57%

Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Slightly more than one-third (34 percent) of C-levels expect their spending on personnel to increase over the next 12 months. Also, 31 percent of C-levels predict increased spending on education and training.

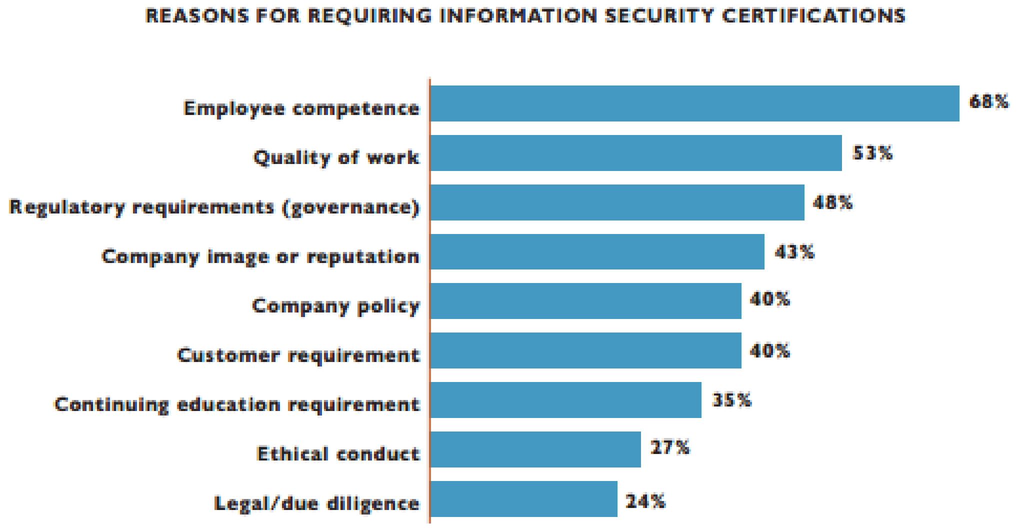
Skills

Across the entire survey, broad understanding of the security field was on top in terms of importance, followed by communication skills. Technical knowledge, awareness and understanding of the latest security threats round out the top four.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Respondents in the banking, finance, and insurance verticals place a higher emphasis on the importance of broad understanding than other verticals. Info tech and government-defense place higher importance on technical knowledge. Healthcare respondents rate communication skills higher in importance. Certification Slightly more than 46 percent of all survey respondents indicated that their organizations require certification, and among those respondents, 50 percent of member and 39 percent of non-member indicate certification is a requirement. Government-defense is most emphatic on this point; 84 percent state certification is required, and a distant, but still high, second is info tech at 47 percent. While regulations are a primary driver for certification in government-defense, that is an anomaly. The private sector overwhelmingly (74 percent) views certification as an indicator of competency. The correlated quality of work was the second highest reason.



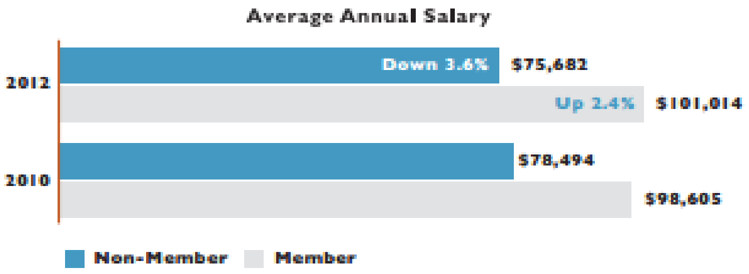
Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

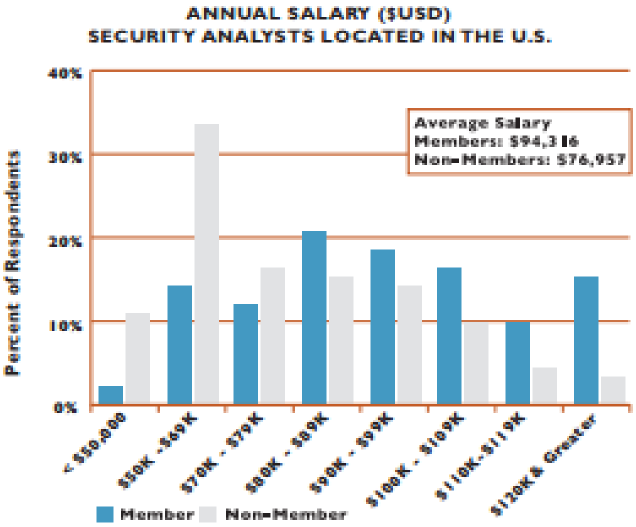
Information Security is a Rewarding and Resilient Profession

The importance of the information security profession has been clearly articulated in this survey by the respondents, which does include bias as they have chosen this career. To gain a more unbiased confirmation of the importance of this profession, the survey asked respondents to weigh in on the uniform measuring sticks of all careers: salary, change in salary, and job stability. In terms of salary, the average annual salary across all survey respondents is US$92,835.

As expected, C-levels and officers reported the highest average annual salary at US$106,151. The respondents in government-defense and healthcare reported the highest average annual salaries at US$101,246 and US$98,037, respectively. In comparing average annual salaries for members and non-members between the 2013 and 2011 surveys, the member average salary is higher, and the salary gap between members and non-members is widening.

Recognizing that many factors influence salary—job title, location, security certifications, and tenure—a narrower examination on salary is appropriate. To gain the greatest confidence possible in salary comparisons with the survey data, we selected the job title and location with the greatest number of respondents: security analyst located in the U.S. As displayed, U.S.-based security analysts that are (ISC)2 members, on average, have a higher salary—23 percent greater than U.S.-based security analysts that are non-members.



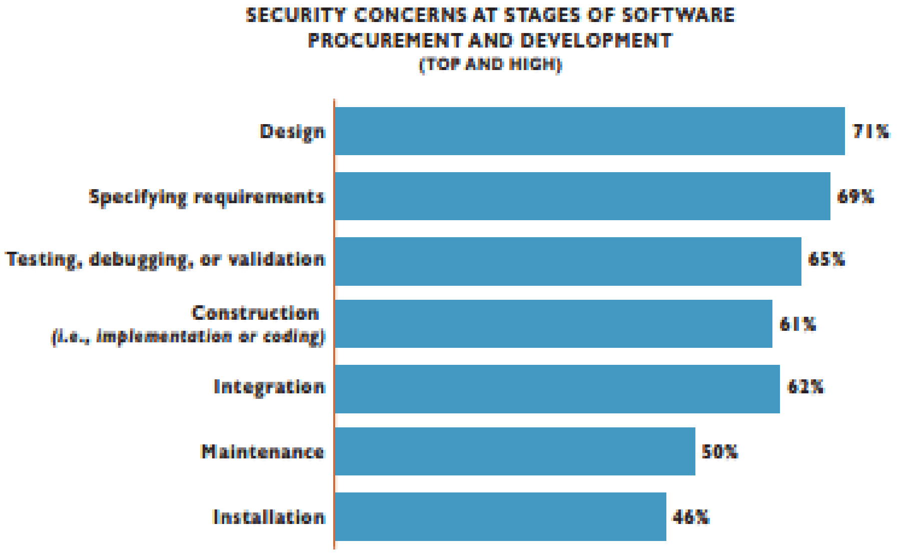


Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Secure Software Development: Essential but Under-Supperted

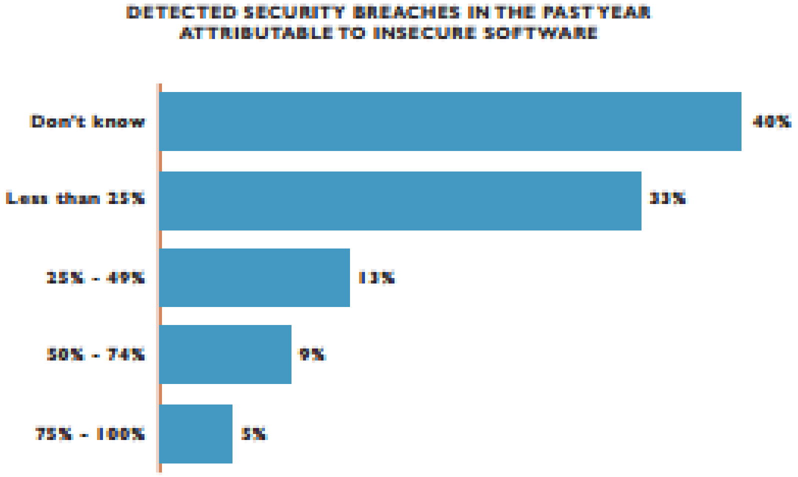
Application vulnerabilities was the number one security concern for survey respondents. Closer examination reveals that the secure software development concern increases with company size, perhaps correlated with the greater amounts of software development in large companies versus smaller companies that rely heavily on commercial applications. Also, the importance of secure software development was rated above software and hardware solutions in securing the organization’s infrastructure. Here, too, there is variance associated with company size.

In particular, as company size increases, the importance of secure software development relative to the importance of software and hardware solutions also increases. Recognizing that software procurement and development involves multiple phases, the level of security concern may fluctuate among these steps. According to the survey respondents, this is true but within a fairly narrow range in the pre-installation steps.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

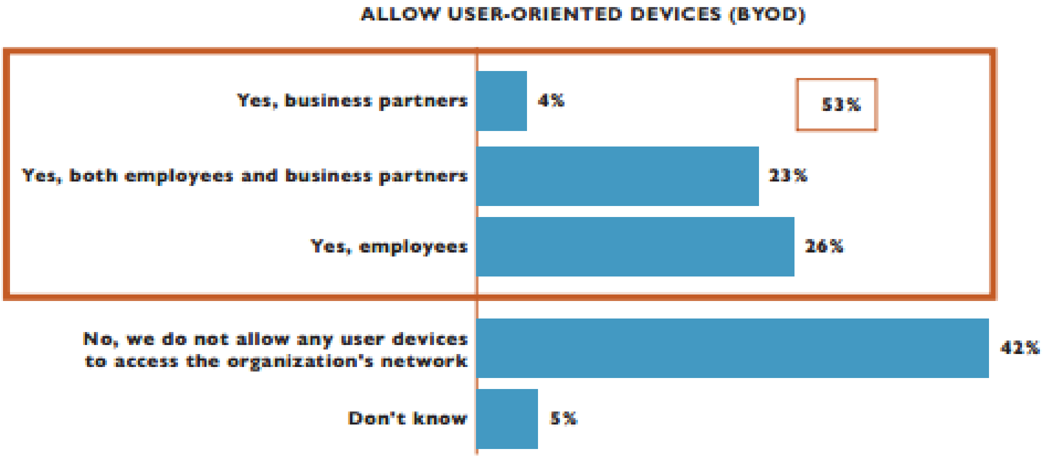
T he risk implications of these concerns are most notable in the proportion of detected security breaches attributed to insecure software. According to survey respondents, insecure software was a contributor in approximately one-third of the 60 percent of detected security breaches. In the other 40 percent of detected breaches, insecure software's role was uncertain either because post-breach forensics were inconclusive, or the survey respondents were not privy to the forensics. Regardless of this uncertainty, along with insecure software's unquantifiable attribution in undetected breaches, information security professionals are certain that their concerns regarding insecure software are justified.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

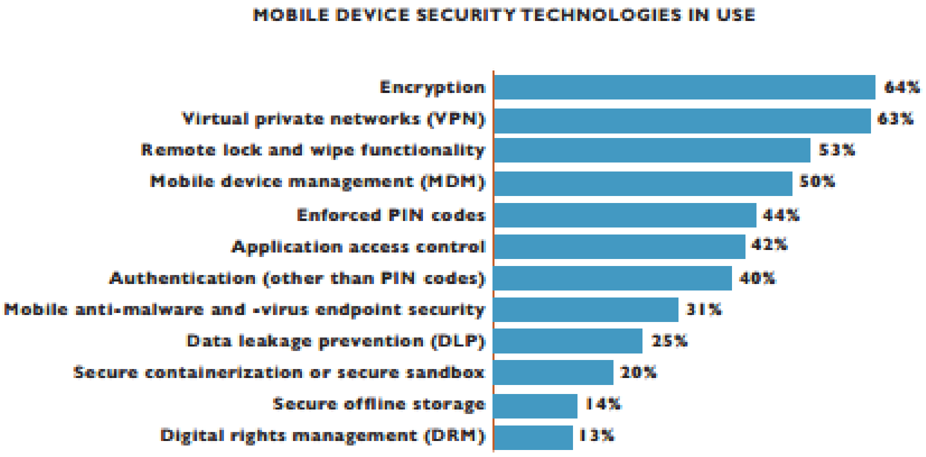
BYOD

Approval for use of user-owned devices, according to this survey, is more than 50 percent. Differences in allowance do exist, primarily among verticals. For example, 67 percent of respondents in government state user-owned devices are not allowed. In the private sector, 47 percent of respondents in banking, insurance, and finance verticals state user-owned devices are not allowed. At the other end, education is most permissive, with 86 percent of education respondents claiming user-owned devices (employee and business partners combined) are allowed



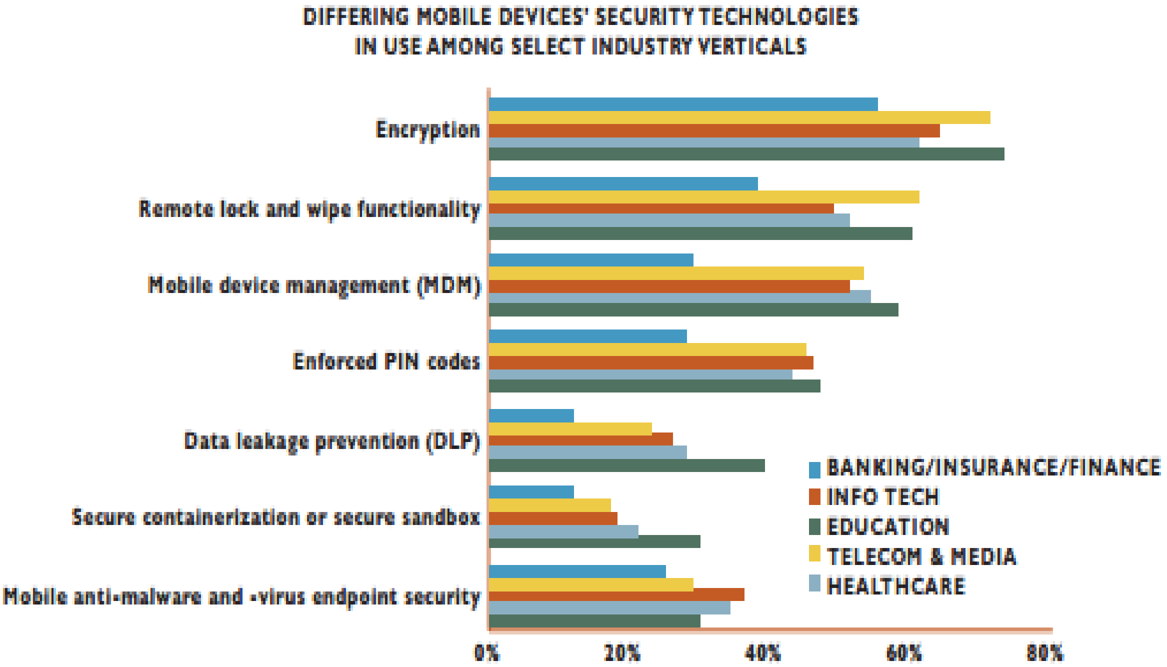
Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

End-user license agreements are one way that companies manage BYOD risk. Fifty-one percent of survey respondents claim agreements are in use. Beyond these agreements, a growing number of security technologies are used. Furthermore, all mobile security technologies listed in the 2011 survey (encryption, remote lock and wipe, MDM, mobile anti-malware, and DRM) had a greater percent of respondents claiming use in 2013. Also as a sign of expanding security technologies in use are the modest percentages assigned to technologies that were in their commercial infancy in 2011, such as secure containerization or secure sandbox, with 20 percent of respondents stating it is used in the 2013 survey.



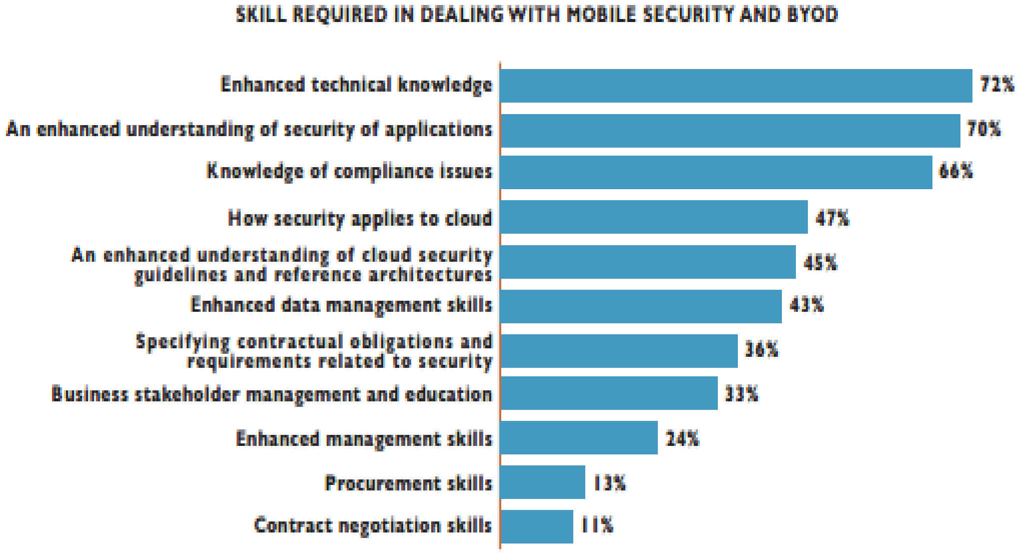
Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Another interesting perspective revealed in the survey is how mobile security technology use varies among industry verticals. The chart below shows differences for five verticals, including the most permissive allowance of user-owned devices vertical (education) and the most restrictive (banking, insurance, and finance). Note: Only mobile security technologies that had use differences of 10 percentage points or more are shown.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

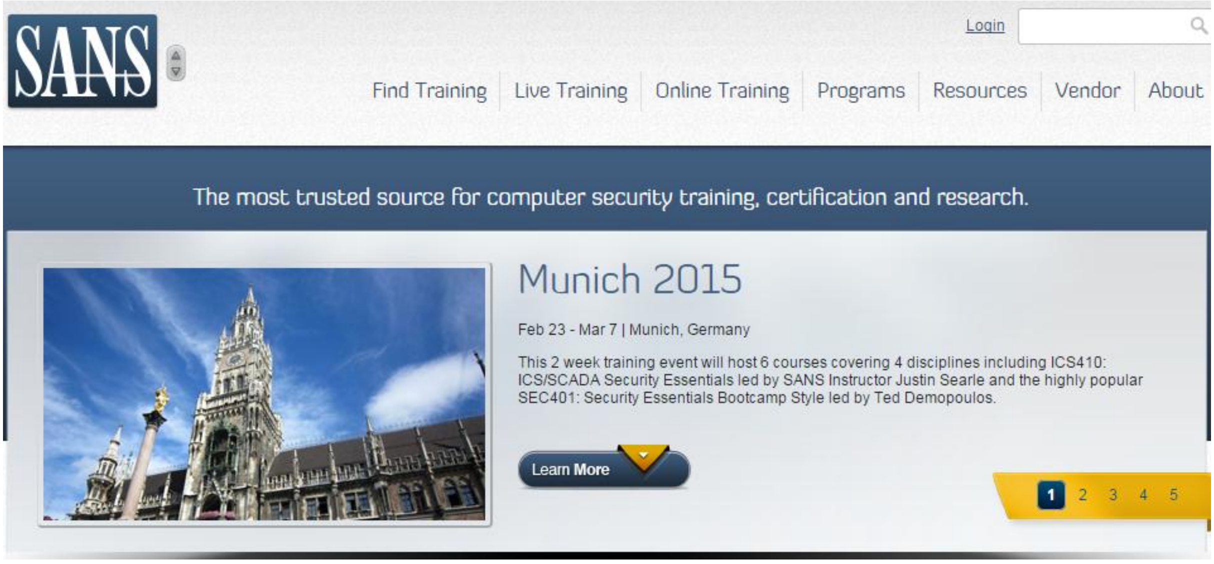
Development of new skills in mobile security and BYOD by information security professionals was noted as required by 74 percent of respondents. This opinion has little variation by company size, job title, or industry vertical. This chart shows which new skills are most required in dealing with mobile security and BYOD.



Source: Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013

Competitors – secure coding training providers

SANS



The most trusted source for computer security training, certification and research.

Munich 2015

Feb 23 - Mar 7 | Munich, Germany

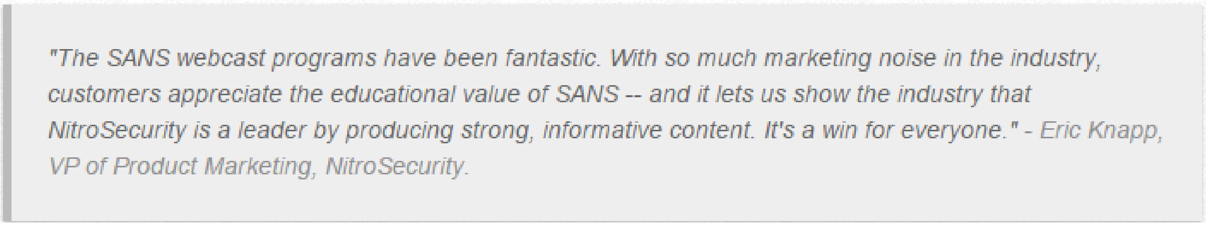
This 2 week training event will host 6 courses covering 4 disciplines including ICS410: ICS/SCADA Security Essentials led by SANS Instructor Justin Searle and the highly popular SEC401: Security Essentials Bootcamp Style led by Ted Demopoulos.

Source: http://www.sans.org/

About SANS:

- Leader in Information Security Training
- Over 165,000 alumni
- 54,000+ GIAC security certifications granted
- Instructors and students are the top guns in information security
- Strong policy and community focus
- Internet Storm Center
- Top 20 Internet Vulnerabilities
- Press/Media Voice
- Research and Analysts
- Industrial Control Systems, DFIR, Penetration Testing and Other Technical Summits
- Consensus Research Projects: 20 Critical Security Controls, Top 25 Software Errors
- Free Resources: Information Security Reading Room, Security Newsletters
- Vendor neutral
- Deep rooted trust position
- Training ground for next-generation of information security and business leaders

> *"After working with SANS for a few years now, the audience at SANS events and webinars continues to represent some of the most forward thinking IT security practitioners looking for new ideas and realworld solutions to mitigate today's modern malware. SANS events and programs are also very professionally managed, which allows us to focus on providing the most engaging content that in turn brings us strong, qualified prospects." - Phillip Lin, Director of Marketing, FireEye*



> *"The SANS webcast programs have been fantastic. With so much marketing noise in the industry, customers appreciate the educational value of SANS -- and it lets us show the industry that NitroSecurity is a leader by producing strong, informative content. It's a win for everyone." - Eric Knapp, VP of Product Marketing, NitroSecurity.*

The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.

Computer Security Training & Certification

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited. The courses are full of important and immediately useful techniques that you can put to work as soon as you return to your offices. They were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and awareness, and the in-depth technical aspects of the most crucial areas of IT security.

SANS training can be taken in a classroom setting from SANS-certified instructors, self-paced over the Internet, or in mentored settings in cities around the world. Each year, SANS programs educate more than 12,000 people in the US and internationally. To find the best teachers in each topic in the world, SANS runs a continuous competition for instructors. Last year more than 90 people tried out for the SANS faculty, but only five new people were selected.

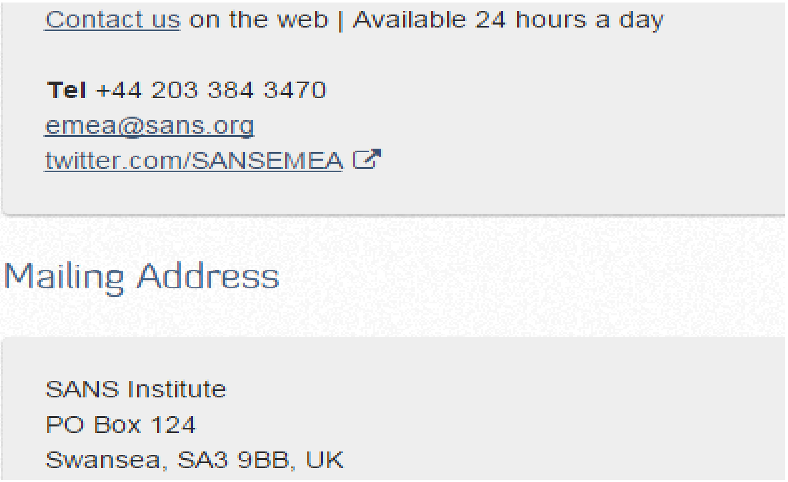
SANS also offers a Work Study Program through which, in return for acting as an important extension of SANS' conference staff, facilitators may attend classes at a greatly reduced rate. Facilitators are most definitely expected to pull their weight and the educational rewards for their doing so are substantial.

Information Security Training - More than 400 multi-day courses in 90 cities around the world

The GIAC Certification Program - Technical certification for people you trust to protect your systems

Information Security Research

- Many of the valuable SANS resources are free to all who ask. They include the very popular Internet Storm Center (the Internet's early warning system), the weekly news digest (NewsBites), the weekly vulnerability digest (@RISK), and more than 1,200 award-winning, original information security research papers.
- SANS Information Security Reading Room - More than 2270 original research papers in 84 important categories of security
- SANS Weekly Bulletins and Alerts - Definitive updates on security news and vulnerabilities
- SANS Security Policy Project - Free Security Policy Templates - Proven in the real world
- Vendor Related Resources - Highlighting the vendors that can help make security more effective
- Information Security Glossary - Words, acronyms, more
- Internet Storm Center - The Internet's Early Warning System
- S.C.O.R.E. - Helping the security community reach agreement on how to secure common software and systems
- SANS/FBI Annual Top 20 Internet Security Vulnerabilities List - A consensus list of vulnerabilities that require immediate remediation
- Intrusion Detection FAQ - Frequently asked questions and answers about intrusion detection
- SANS Press Room - Our press room is designed to assist the media in coverage of the information assurance industry



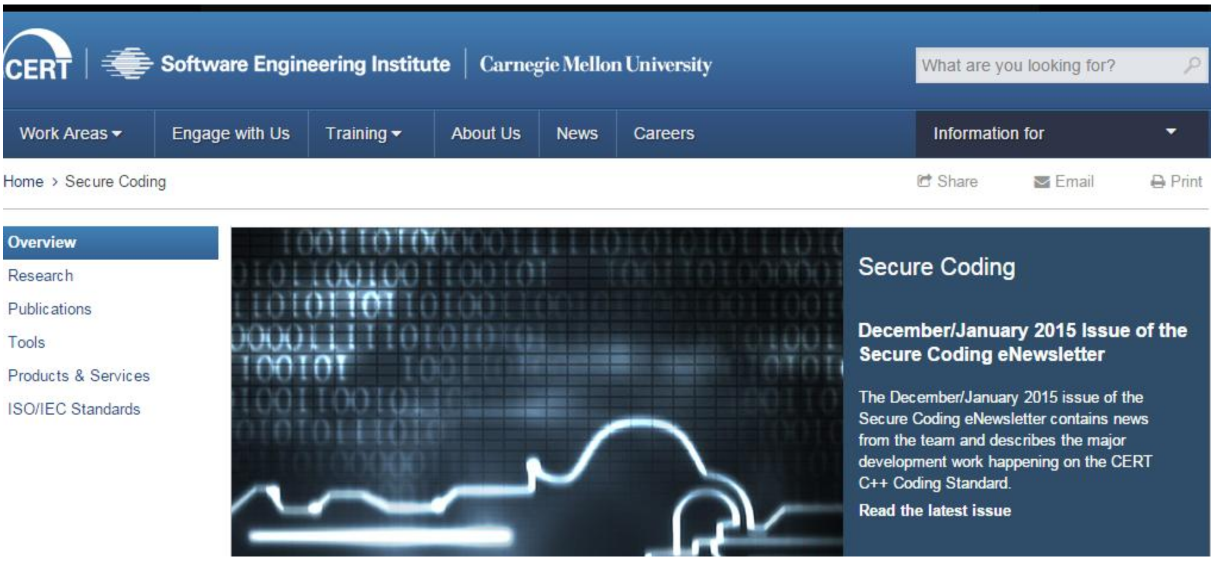
Contact us on the web | Available 24 hours a day

Tel +44 203 384 3470
emea@sans.org
twitter.com/SANSEMEA

Mailing Address

SANS Institute
PO Box 124
Swansea, SA3 9BB, UK

CERT



Secure Coding

December/January 2015 Issue of the Secure Coding eNewsletter

The December/January 2015 issue of the Secure Coding eNewsletter contains news from the team and describes the major development work happening on the CERT C++ Coding Standard.

Read the latest issue

http://www.cert.org/secure-coding/

About CERT

Begun with a simple handshake and a fundamental mission, the CERT Division of the Software Engineering Institute (SEI) has evolved dramatically since it was created in 1988 as the CERT Coordination Center in response to the Morris worm incident. The small organization established to coordinate response to internet security incidents now has more than 150 cybersecurity professionals working on projects that take a proactive approach to securing systems.

Recognized as a trusted, authoritative organization dedicated to improving the security and resilience of computer systems and networks, the CERT Division is a national asset in the field of cybersecurity. We regularly partner with government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats.

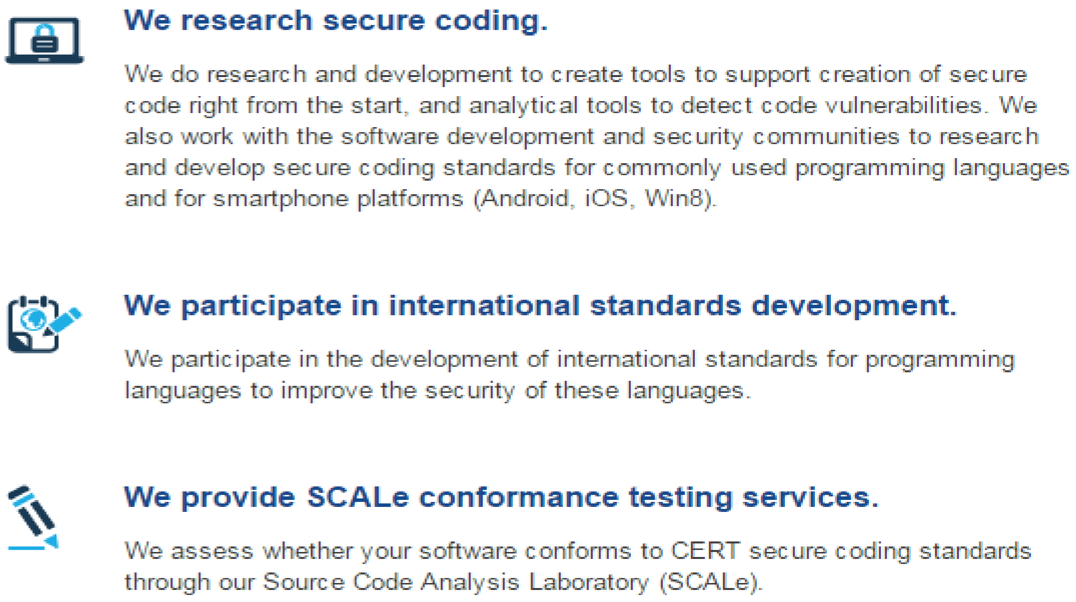
The CERT Division is enriched by its connection to the internationally respected Carnegie Mellon University. Our proximity to other world-class researchers and practitioners enables numerous collaboration opportunities and strengthens our research focus. And because the CERT Division is located within the SEI, a federally funded research and development center at Carnegie Mellon University, the majority of our work contributes to government and national security efforts.

The CERT Division works closely with the Department of Homeland Security (DHS) to meet mutually set goals in areas such as data collection and mining, statistics and trend analysis, computer and network security, incident management, insider threat, software assurance, and more. The results of this work include exercises, courses, and systems that were designed, implemented, and delivered to DHS and its customers as part of the SEI's mission to transition SEI capabilities to the public and private sectors and improve the practice of cybersecurity.

We reduce the number of vulnerabilities to a level that can be fully mitigated in operational environments. This reduction is accomplished by preventing coding errors or discovering and eliminating security flaws during implementation and testing.

The CERT Division has been extremely successful in the development of secure coding standards, which have been adopted at corporate levels by companies such as Cisco and Oracle, and the development of the Source Code Analysis Laboratory (SCALe), which supports conformance testing of systems against these coding standards. The success of the secure coding standards and SCALe contributed to the impetus for including software assurance requirements in the National Defense Authorization Act (NDAA) for Fiscal Year 2013.

Eliminating vulnerabilities during development can result in a two to three orders-of-magnitude reduction in the total cost of repairing the code versus making the repairs afterwards. To achieve these goals, it is necessary to determine how to develop verifiably secure code within budget and on schedule.



We research secure coding.

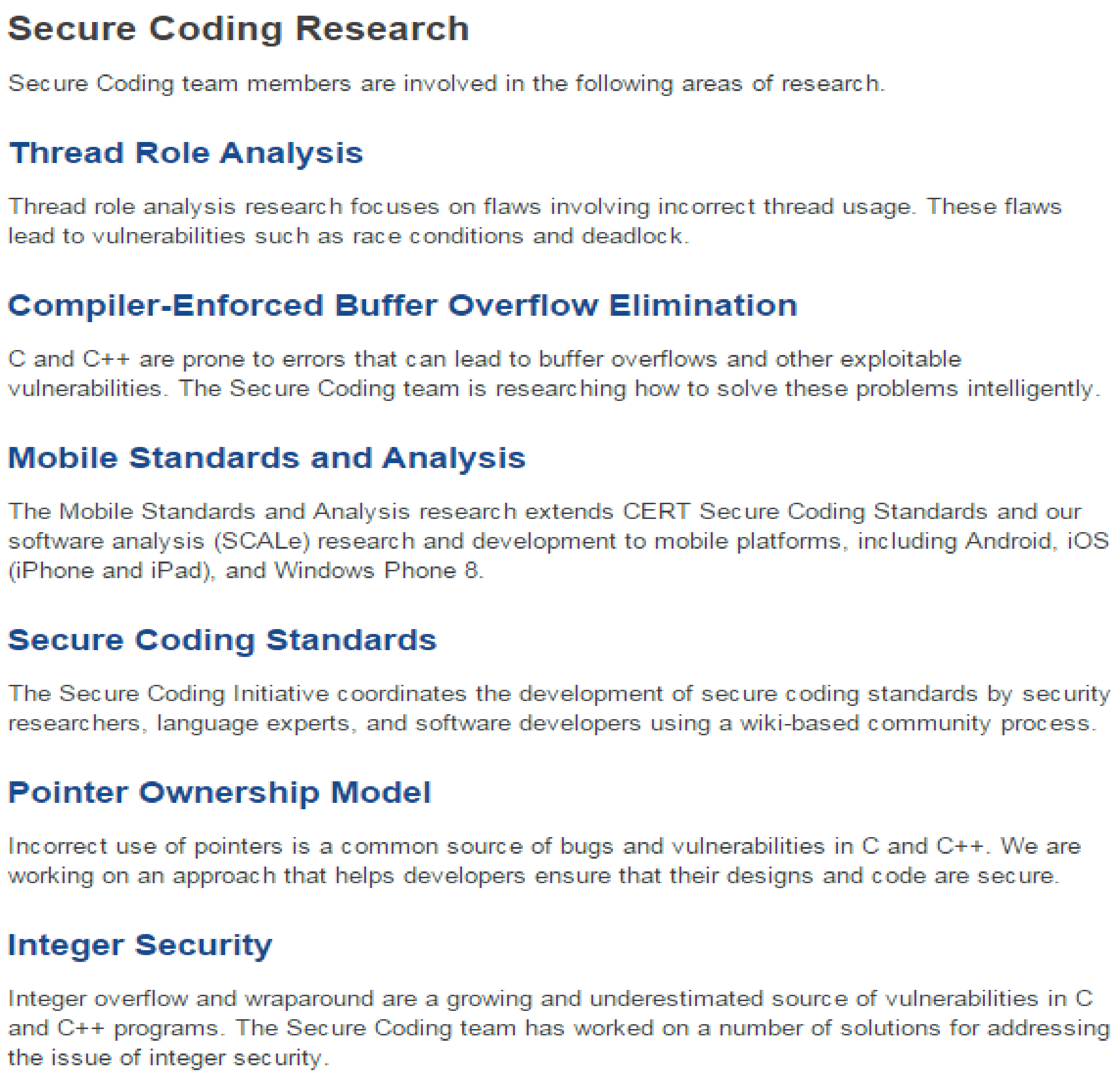
We do research and development to create tools to support creation of secure code right from the start, and analytical tools to detect code vulnerabilities. We also work with the software development and security communities to research and develop secure coding standards for commonly used programming languages and for smartphone platforms (Android, iOS, Win8).

We participate in international standards development.

We participate in the development of international standards for programming languages to improve the security of these languages.

We provide SCALe conformance testing services.

We assess whether your software conforms to CERT secure coding standards through our Source Code Analysis Laboratory (SCALe).



Secure Coding Research

Secure Coding team members are involved in the following areas of research.

Thread Role Analysis

Thread role analysis research focuses on flaws involving incorrect thread usage. These flaws lead to vulnerabilities such as race conditions and deadlock.

Compiler-Enforced Buffer Overflow Elimination

C and C++ are prone to errors that can lead to buffer overflows and other exploitable vulnerabilities. The Secure Coding team is researching how to solve these problems intelligently.

Mobile Standards and Analysis

The Mobile Standards and Analysis research extends CERT Secure Coding Standards and our software analysis (SCALe) research and development to mobile platforms, including Android, iOS (iPhone and iPad), and Windows Phone 8.

Secure Coding Standards

The Secure Coding Initiative coordinates the development of secure coding standards by security researchers, language experts, and software developers using a wiki-based community process.

Pointer Ownership Model

Incorrect use of pointers is a common source of bugs and vulnerabilities in C and C++. We are working on an approach that helps developers ensure that their designs and code are secure.

Integer Security

Integer overflow and wraparound are a growing and underestimated source of vulnerabilities in C and C++ programs. The Secure Coding team has worked on a number of solutions for addressing the issue of integer security.

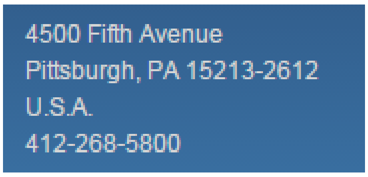
Courses by Topic

CERT training is offered in the following areas:

Incident Handling

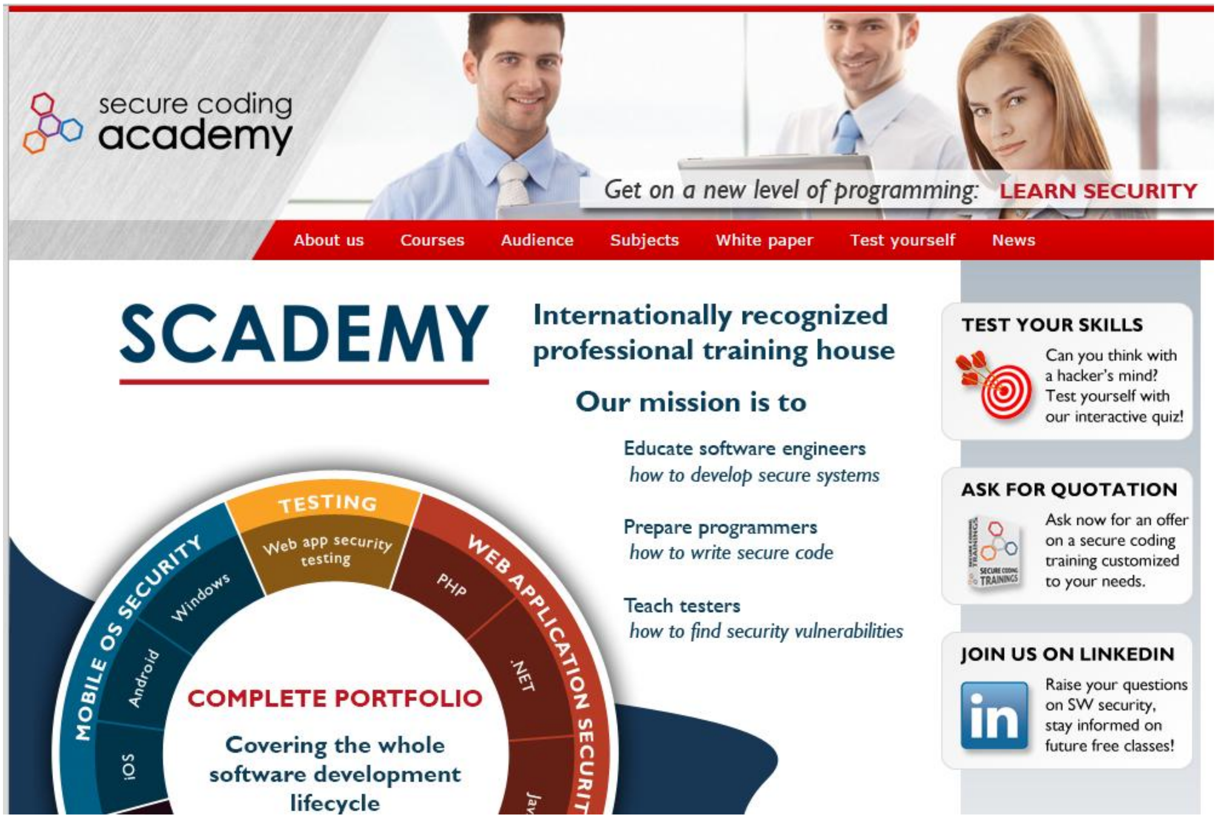
Network Security

Risk Assessment & Insider Threat



4500 Fifth Avenue
Pittsburgh, PA 15213-2612
U.S.A.
412-268-5800

Secure Coding Academy



Internationally recognized professional training house

Our mission is to

Educate software engineers
how to develop secure systems

Prepare programmers
how to write secure code

Teach testers
how to find security vulnerabilities

Covering the whole software development lifecycle

TEST YOUR SKILLS

Can you think with a hacker's mind? Test yourself with our interactive quiz!

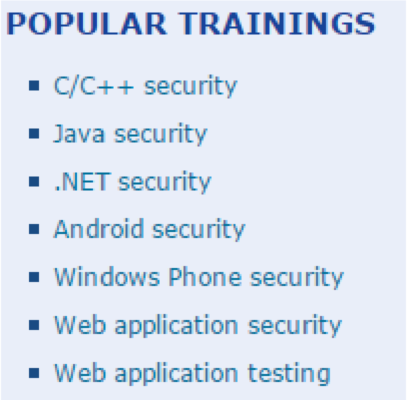
ASK FOR QUOTATION

Ask now for an offer on a secure coding training customized to your needs.

JOIN US ON LINKEDIN

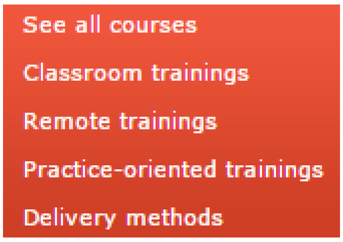
Raise your questions on SW security, stay informed on future free classes!

Source: http://www.securecodingacademy.com/

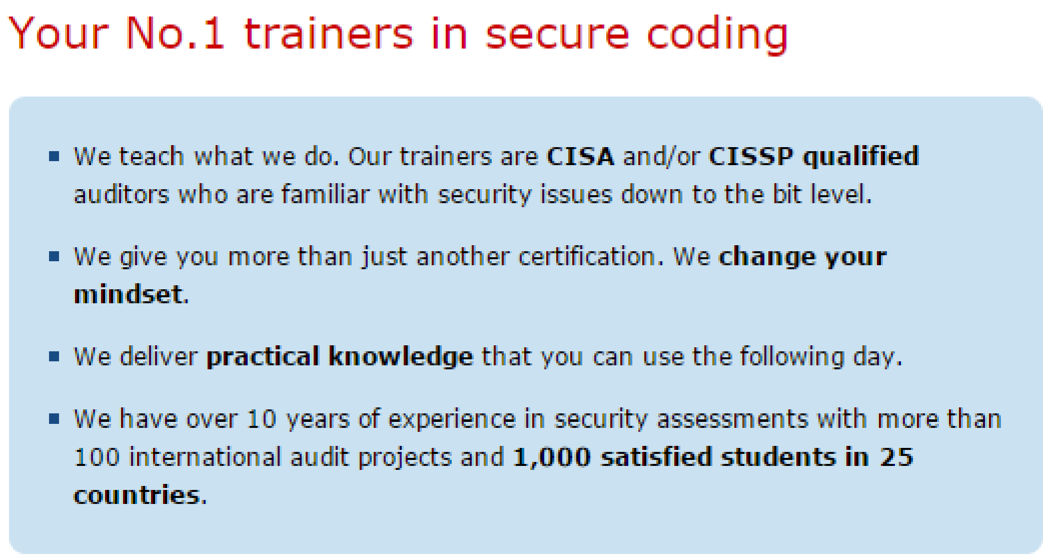


POPULAR TRAININGS

- C/C++ security
- Java security
- .NET security
- Android security
- Windows Phone security
- Web application security
- Web application testing



See all courses
Classroom trainings
Remote trainings
Practice-oriented trainings
Delivery methods



Your No.1 trainers in secure coding

- We teach what we do. Our trainers are **CISA** and/or **CISSP qualified** auditors who are familiar with security issues down to the bit level.
- We give you more than just another certification. We **change your mindset**.
- We deliver **practical knowledge** that you can use the following day.
- We have over 10 years of experience in security assessments with more than 100 international audit projects and **1,000 satisfied students in 25 countries**.

10 years of experience

In the last decade we have earned outstanding international market recognition in security analysis, audit and testing of security-sensitive products, with customers coming from various industrial segments and all continents. Stemming from the academic roots and based on strong software security expertise, since 2005 our services are complemented with the SEARCH-LAB Secure Coding Academy**,**offering a set of practical courses that are specifically designed to serve corporate software development groups.

- **Practice-oriented** trainings coming with a lots of easy-to-understand examples
- **Hands-on exercises** providing live hacking fun to support full understanding of the risks
- **Didactic** courses backed by more than a decade of teaching experience
- **Up-to-date** on current trends in attack methods and mitigation techniques
- **State-of-the art** research results continuously incorporated into the learning materials

Professional activities

With our presence in various industrial initiatives we are not only following, but also actively leveraging the state of the art in secure coding. Some of such secure software development initiatives include:

SAFECODE – dedicated to increasing trust in ICT products, funded by the biggest software developing companies like Microsoft, SAP, Nokia or Adobe.

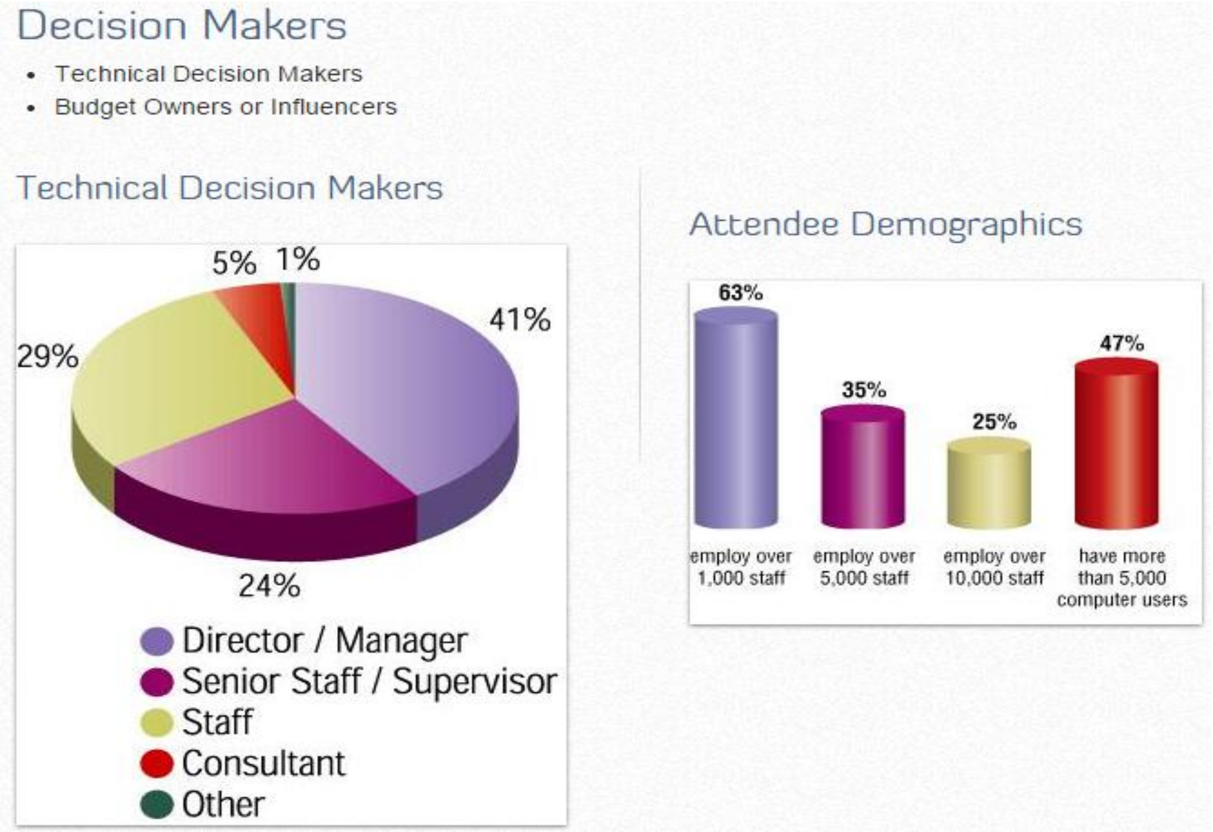
SHIELDS – aims at detecting security problems from within design and development tools, operating a machine-readable Software Vulnerability Repository.

Other secure coding providers:

- http://www.infosecinstitute.com/courses/secure-coding.html
- https://training.safecode.org/
- https://www.fishnetsecurity.com/6labs/resource-library/white-paper/secure-code-training
- https://www.owasp.org/index.php/OWASP/Training/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
- http://www.denimgroup.com/application-security-training.html
- http://www.sei.cmu.edu/training/P63.cfm
- https://security.berkeley.edu/content/application-software-security-guidelines
- https://www.whitehatsec.com/edu/onsite/java.html
- http://oli.cmu.edu/courses/future-2/secure-coding-course-details/
- http://www.giac.org/certification/secure-software-programmer-java-gssp-java
- https://www.develop.com/training-course/secure-java-coding
- http://www.cigital.com/training/
- http://www.cenzic.com/services-support/training/best-practices-for-secure-coding/
- http://services.geant.net/multidomainsecurity/Resources/Documents/Security_training_leaflet.pdf
- https://appsec-labs.com/training/
- http://clearskies.net/secure_code.php
- http://www.securestate.com/Services/Risk%20Management/Pages/Secure-Coding-Practices.aspx
- http://www.inspiredelearning.com/courses/secure-programming/

Attendee Profile & Demographic Information[9]

Attending a SANS conference costs most attendees more than $4000 for tuition. Add the cost of hotel, travel, and time away from the office, and you can appreciate that the companies sending people to SANS are making a substantial investment in their education. They are not the same old people attending a free breakfast. They are the most qualified audience of decision makers and technical influencers you can find.



Decision Makers

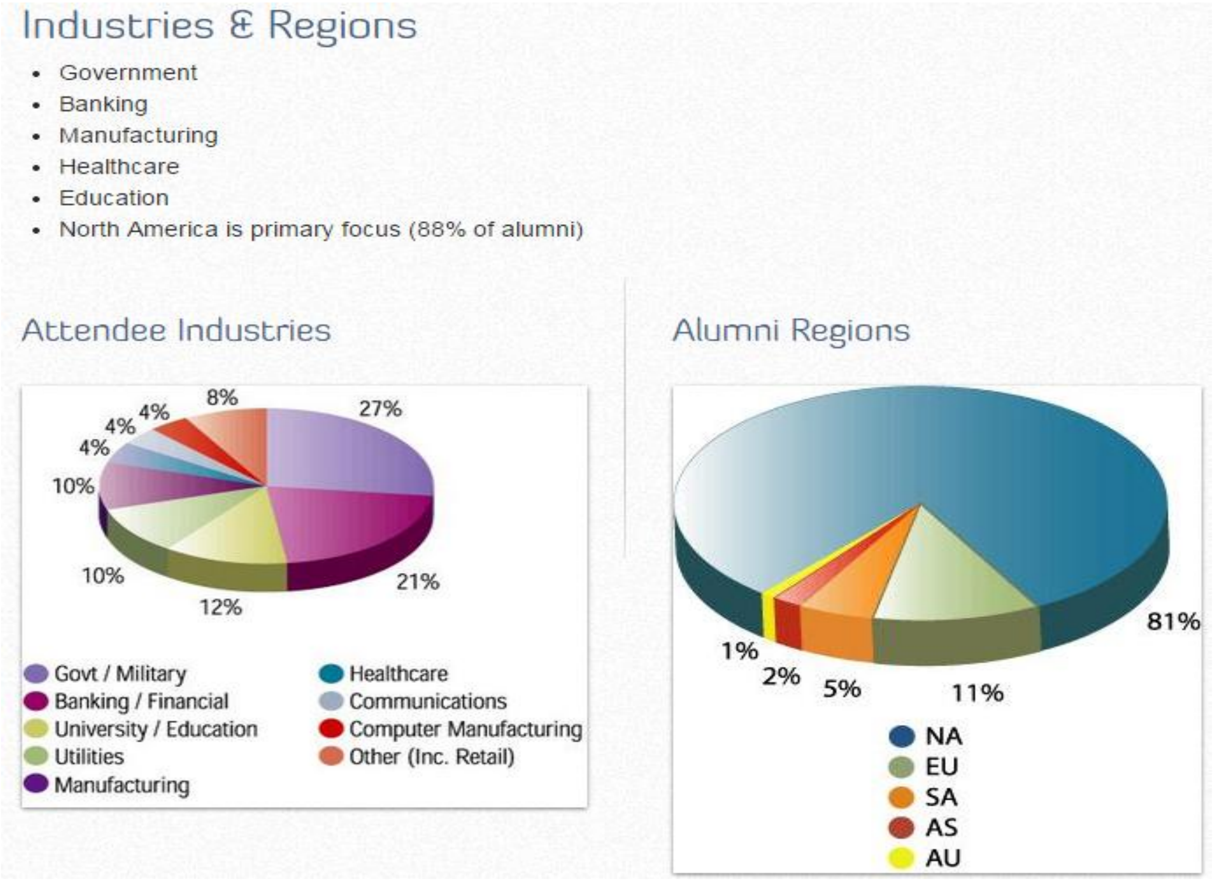
- Technical Decision Makers
- Budget Owners or Influencers

Technical Decision Makers

Attendee Demographics

Source: http://www.sans.org/vendor/demographics/

[9] Source: http://www.sans.org/vendor/demographics/



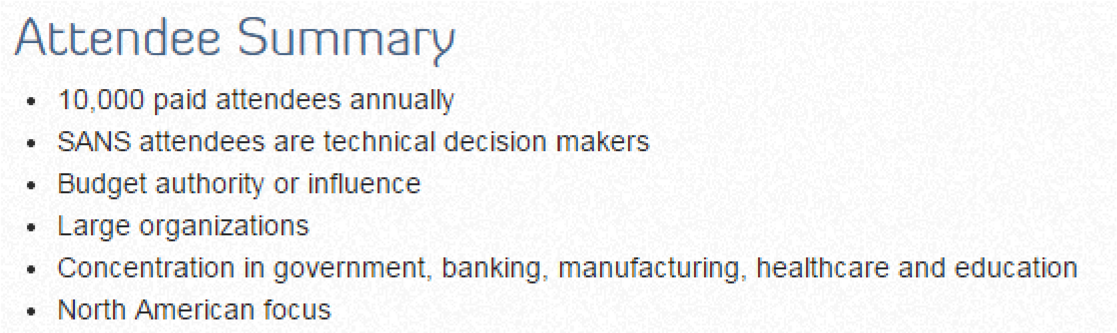
Industries & Regions

- Government
- Banking
- Manufacturing
- Healthcare
- Education
- North America is primary focus (88% of alumni)

Attendee Industries

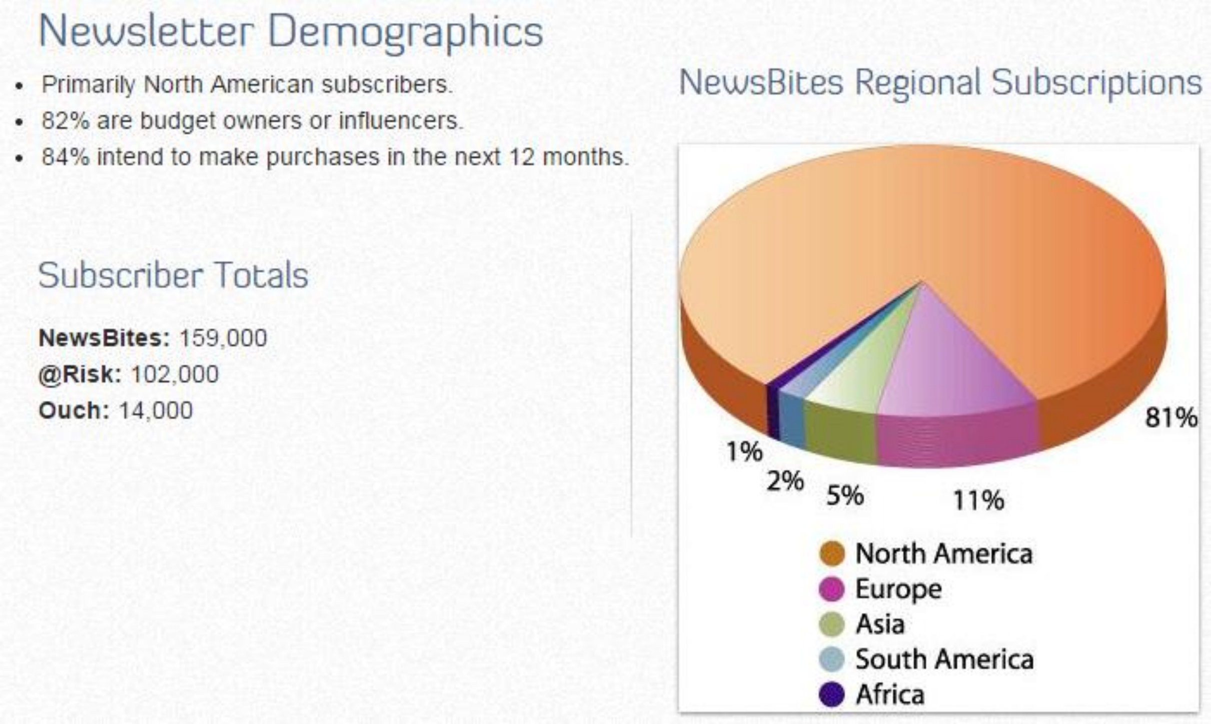
Alumni Regions

Source: http://www.sans.org/vendor/demographics/



Attendee Summary

- 10,000 paid attendees annually
- SANS attendees are technical decision makers
- Budget authority or influence
- Large organizations
- Concentration in government, banking, manufacturing, healthcare and education
- North American focus



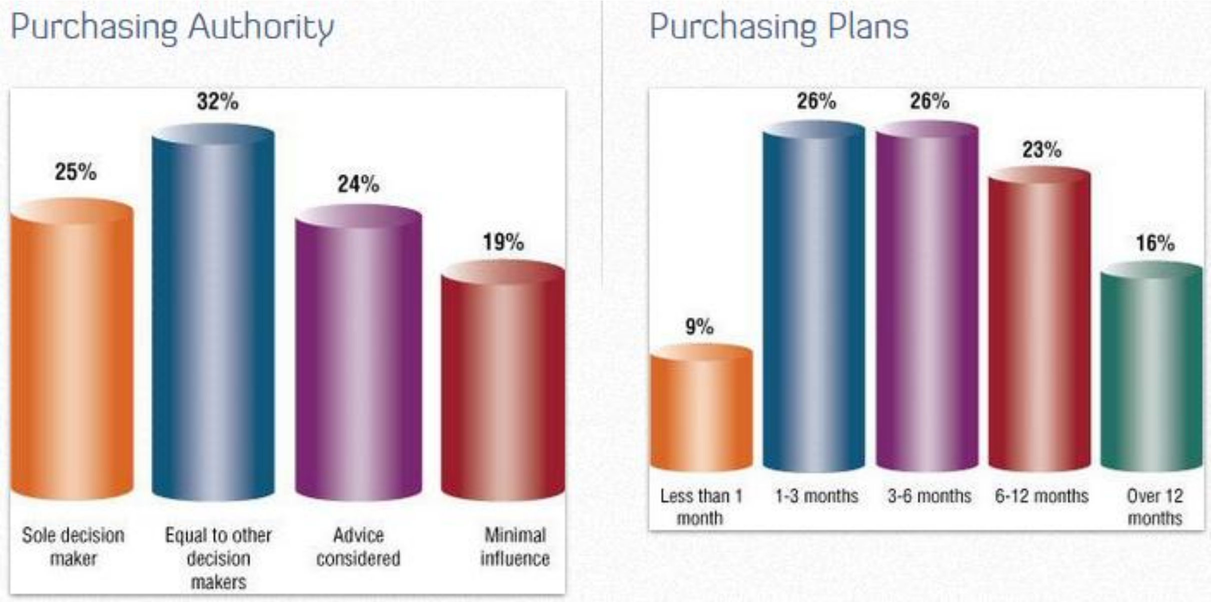
Newsletter Demographics

- Primarily North American subscribers.
- 82% are budget owners or influencers.
- 84% intend to make purchases in the next 12 months.

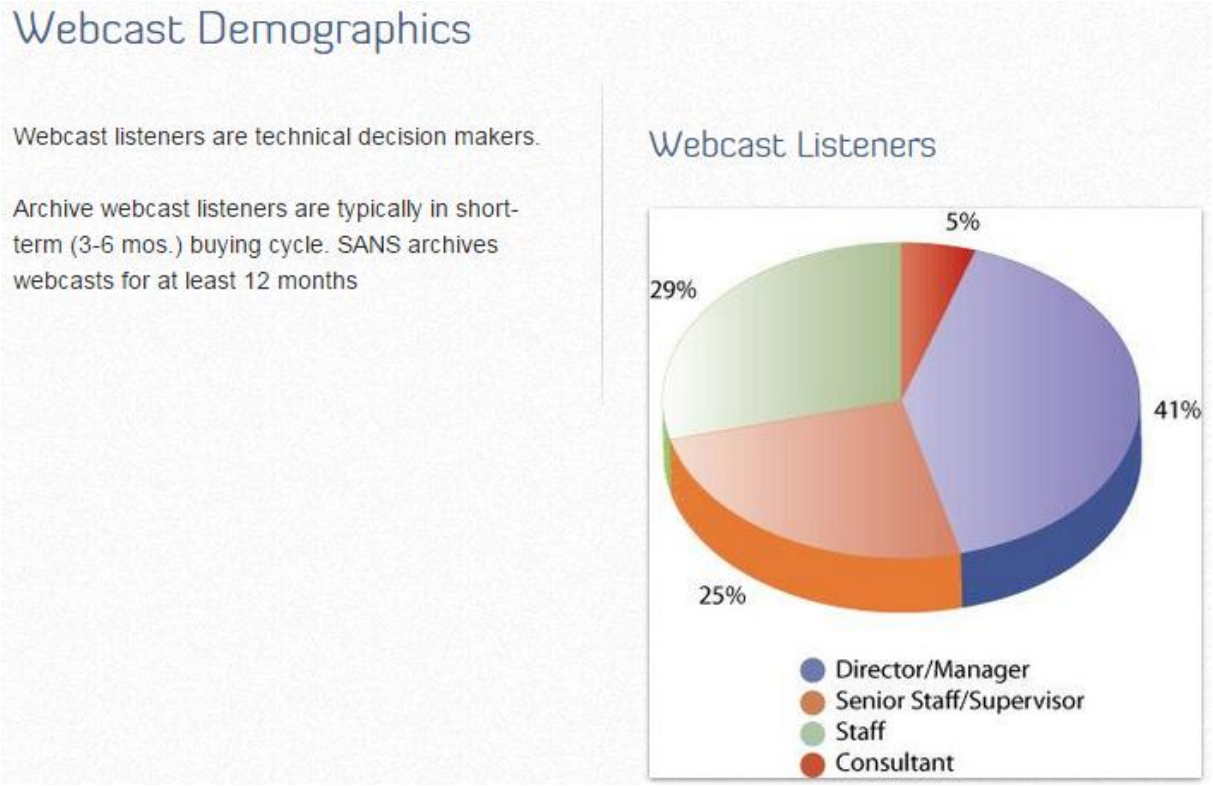
Subscriber Totals

NewsBites: 159,000
@Risk: 102,000
Ouch: 14,000

Source: http://www.sans.org/vendor/demographics/



Source: http://www.sans.org/vendor/demographics/

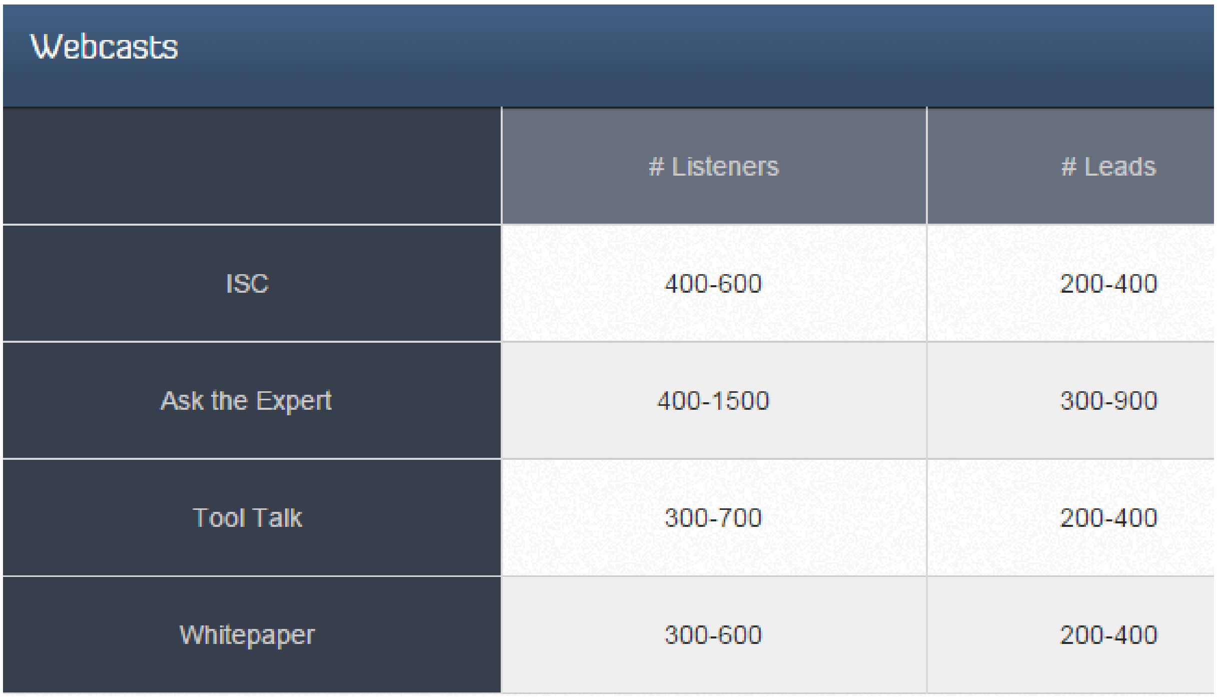


Webcast Demographics

Webcast listeners are technical decision makers.

Archive webcast listeners are typically in short-term (3-6 mos.) buying cycle. SANS archives webcasts for at least 12 months

Source: http://www.sans.org/vendor/demographics/



Webcasts

	# Listeners	# Leads
ISC	400-600	200-400
Ask the Expert	400-1500	300-900
Tool Talk	300-700	200-400
Whitepaper	300-600	200-400

Source: http://www.sans.org/vendor/demographics/

Sources:

- http://www.securecodingacademy.com/documents/10739/0/SW%20Security%20facts%20and%20misc%20WHITE%20PAPER
- http://www.gartner.com/newsroom/id/2512215
- http://www.gartner.com/newsroom/id/2828722
- http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128
- http://www.statista.com/
- http://smart-grid.tmcnet.com/topics/smart-grid/articles/2013/04/04/333033-smart-grid-cyber-security-faces-funding-challenges.htm
- http://www.sans.org/
- http://www.cert.org/secure-coding/
- http://www.securecodingacademy.com/
- https://www.asisonline.org/News/Press-Room/Press-Releases/2013/Pages/Groundbreaking-Study-Finds-U.S.-Security-Industry-to-be-$350-Billion-Market.aspx
- http://www.slideshare.net/immixGroup/cyber-security-slide-deck
- Michael Suby; The 2013 (ISC)2 Global Information Security Workforce Study, FROST 2013