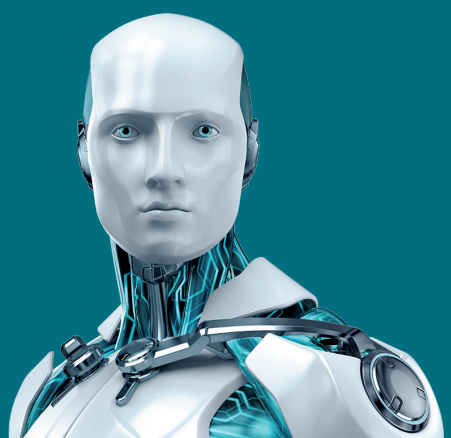
February 2016

BUSINESS SURVEYS 2015

The state of information security in companies in the EMEA region, and the attitudes of their IT experts and managers

ENJOY SAFER TECHNOLOGY™



CONTENTS

EXECUTIVE SUMMARY

This report summarizes the most important findings of a series of recent surveys that ESET has conducted in the EMEA region, focusing on businesses.

One of the most notable findings is that malware infection is reported as the most frequent security incident, mentioned by 58% of all respondents.

The data also prove that almost all companies are trying hard to mitigate cyber security risks by applying various protective systems. Over 98% of all the respondents polled report using at least one security solution, of which antivirus was the most common.

What comes as a surprise is the fact that firms are not paying enough attention to the security of mobile devices, with only 21% of them using a mobile security solution.

The size of the firms also seems to be a significant factor when it comes to the variety of IT security solutions implemented. Bigger firms come out of the poll as more responsible, investing more money in keeping their sensitive data and systems protected.

Another interesting finding is that only 38% of all EMEA respondents consider their company's budget for cyber security to be sufficient.

CYBER SECURITY IN EMEA

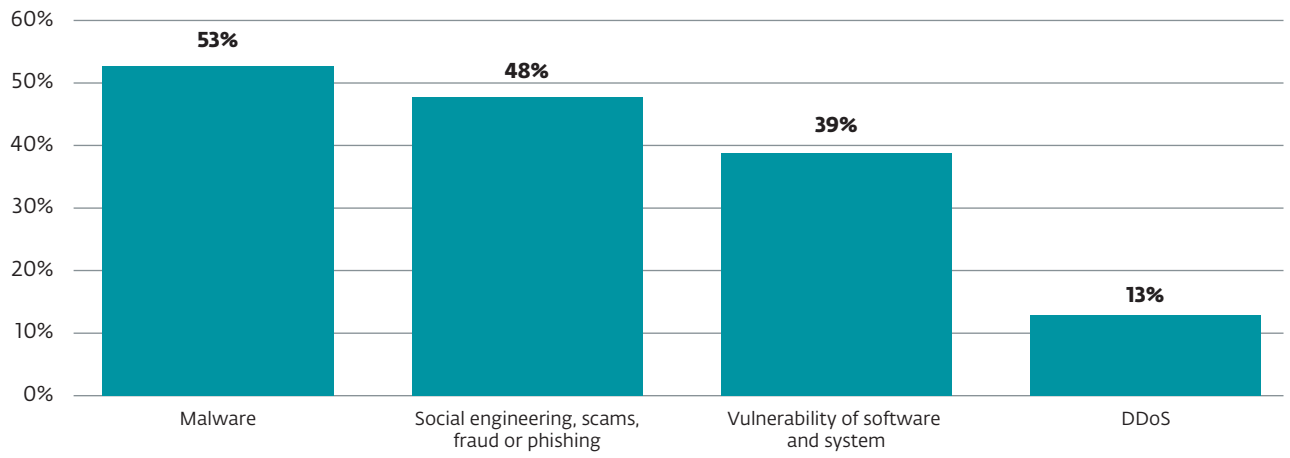
Threats EMEA companies fear the most

What would you expect to be the biggest cyber security concern in the EMEA region? If you put your money on **malware infection**, you would be right. According to ESET's B2B surveys, this threat is responsible for sleepless nights in more than **half of the companies questioned (53%)**.

Social engineering, scams, fraud or phishing ranked second, being mentioned by a little under half of the polled respondents **(48%)**, leaving third place to **vulnerabilities in software and systems (39%)**.

Distributed denial-of-service (DDoS), by which an attacker misuses a network of zombie computers to make repeated requests to one device, causing it to slow down or even crash, has a significantly lower concern rate. Such attacks, designed to down websites or systems, worry close to **one in eight (13%)** of those businesses questioned in the EMEA region, placing it fourth in this category.

What are your biggest IT security concerns?



Incidents experienced by EMEA companies in 2015

As concerns might not precisely reflect reality, we asked EMEA businesses to specify the security incidents they had actually experienced in the previous year.

Their answers show that **79% experienced one or more of the four aforementioned security incidents** during the previous 12 months – (i) malware infection, (ii) social engineering, scams, fraud or phishing, (iii) exploitation of vulnerabilities, or (iv) DDoS attacks.

> *"79% of EMEA companies experienced one or more security incidents during the previous 12 months."*

Detailed statistics reveal that **malware infections** are legitimately sending chills down the spine of IT admins, managers and basically anyone in the EMEA businesses questioned. In just one year, malware caused a security incident in **almost six in ten of the firms polled (58%)**.

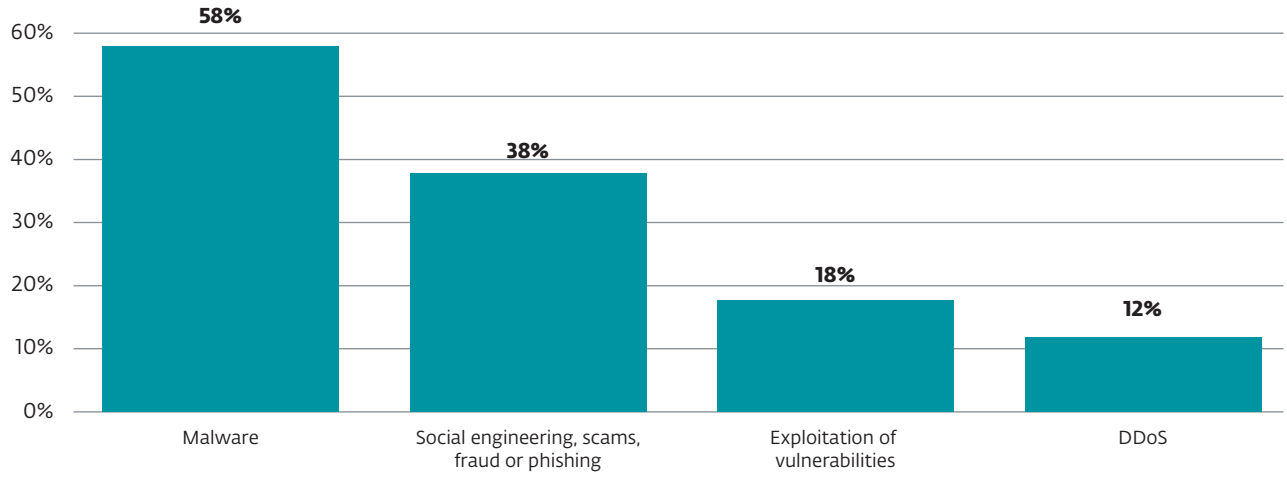
This earns malware the highest position in our ranking, outstripping the second most frequent form of attack – **phishing, scams, social engineering and fraud (38%)** – by more than 20 percent.

Close to one in five EMEA companies report a security incident caused by **exploitation of vulnerabilities (18%)**, rating this threat as the third most widespread in our pool of respondents. One possible explanation for this is that fears connected to system loopholes[1] are leading companies to impose stricter patch and update policies, thereby lowering their impact on company operations.

On the other hand, some of the vulnerabilities and their exploitation by attackers may still be under the radar, making them invisible to the polled companies – and to our statistics as well.

Distributed denial-of-service (DDoS) was the least frequent type of incident **(12%)** seen by businesses polled in the EMEA region in 2015. This number is actually comparable to the level of concern this type of threat raises.

Security incidents experienced in 2015



Antivirus is the most widespread security solution

Focusing on the cyber security measures imposed, it seems that almost all the firms polled by ESET have implemented at least some kind of technological protection for their devices.

More than **98% of them report having one or more of the suggested security solutions** (antivirus, firewall, backup, antispam, authentication of users in the network, intrusion detection or prevention system, two- or multifactor authentication, encryption, mobile security solution) **in place**.

1) http://www.welivesecurity.com/2016/01/26/windows-exploitation-in-2015/

"More than 98% of companies report having one or more of the common security solutions in place."

Detailed information indicates that **antivirus (91%), firewall (85%)** and **backups (77%)** were the three most popular protective systems. Only a negligible portion of respondents (a little over 1%) admitted to having no security measures in place.

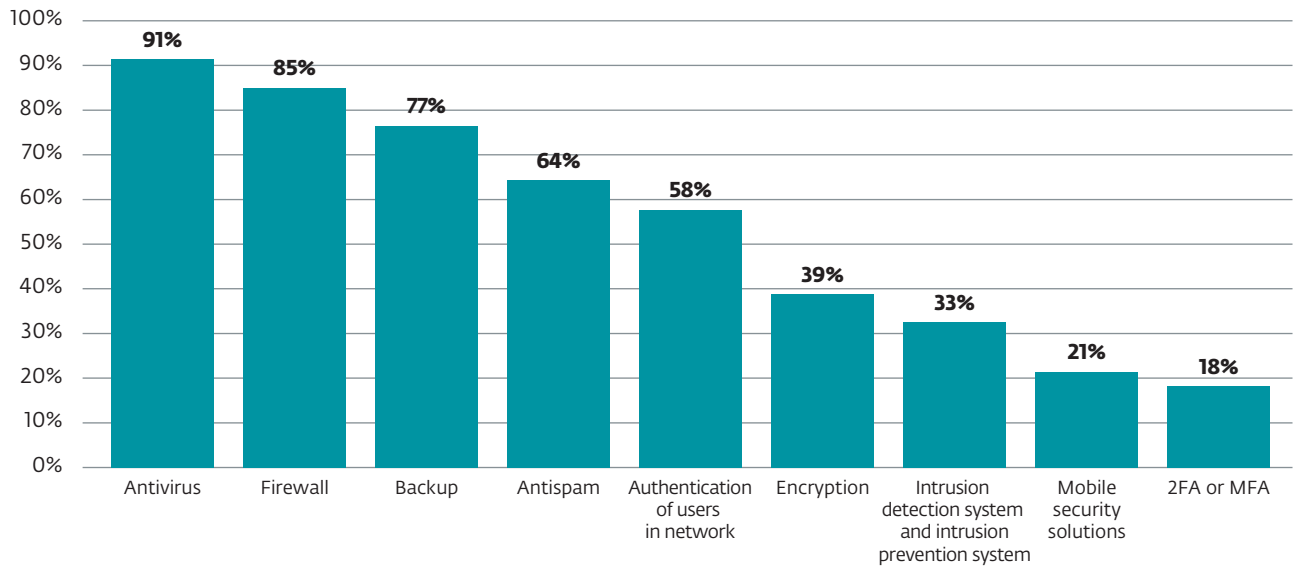
From the options offered, **antispam and authentication of users in the network** were also quite common – applied in close to two-thirds **(64%)** and in over a half **(58%)** of EMEA businesses, respectively.

Unfortunately, the poll showed a lower level of adoption for advanced types of protection. Only just over a third **(39%)** of companies protect their documents by **encrypting** them. An **intrusion detection system or intrusion protection system** is reported to be implemented even less frequently – only by **33%** of EMEA respondents.

Companies in the region which use **two- or multi-factor authentication (2FA or MFA)** are remarkably rare, with only **18%** reporting use of such solutions.

One of the interesting findings was that only **one-fifth** of all polled businesses report using **mobile security solutions (21%)**. With mobile devices being increasingly vulnerable to aggressive malware such as ransomware[2] (and other forms of cyberattacks[3] as well), this might pose a significant risk to companies, their systems and their sensitive data in the near future.

Which of the following security systems do you use in your business?



Neglected mobile security

Another reason why EMEA companies should devote more energy and resources to secure the mobile devices of their employees is the growing number of firms adopting **bring your own device (BYOD)** policies across the region.

ESET's poll has shown that over **four in ten firms (44%) allow** their employees to use their own smartphone, tablet or computer for work-related purposes.

Almost a third of EMEA firms adopt a different policy, trying to mitigate the threat level by **prohibiting BYOD (29%)**. Although this might be perceived as preventive, there might be hidden risks if employees smuggle their private devices into the workplace despite a ban and thus create the feared 'shadow IT'.

2) http://www.welivesecurity.com/2015/09/10/aggressive-android-ransomware-spreading-in-the-usa/
3) http://www.welivesecurity.com/2015/11/06/mobile-security-important-ever/

Estimates[4] say that about 30% to 40% of such smartphones, tablets and computers fly under the company radar and are therefore uncontrollable.

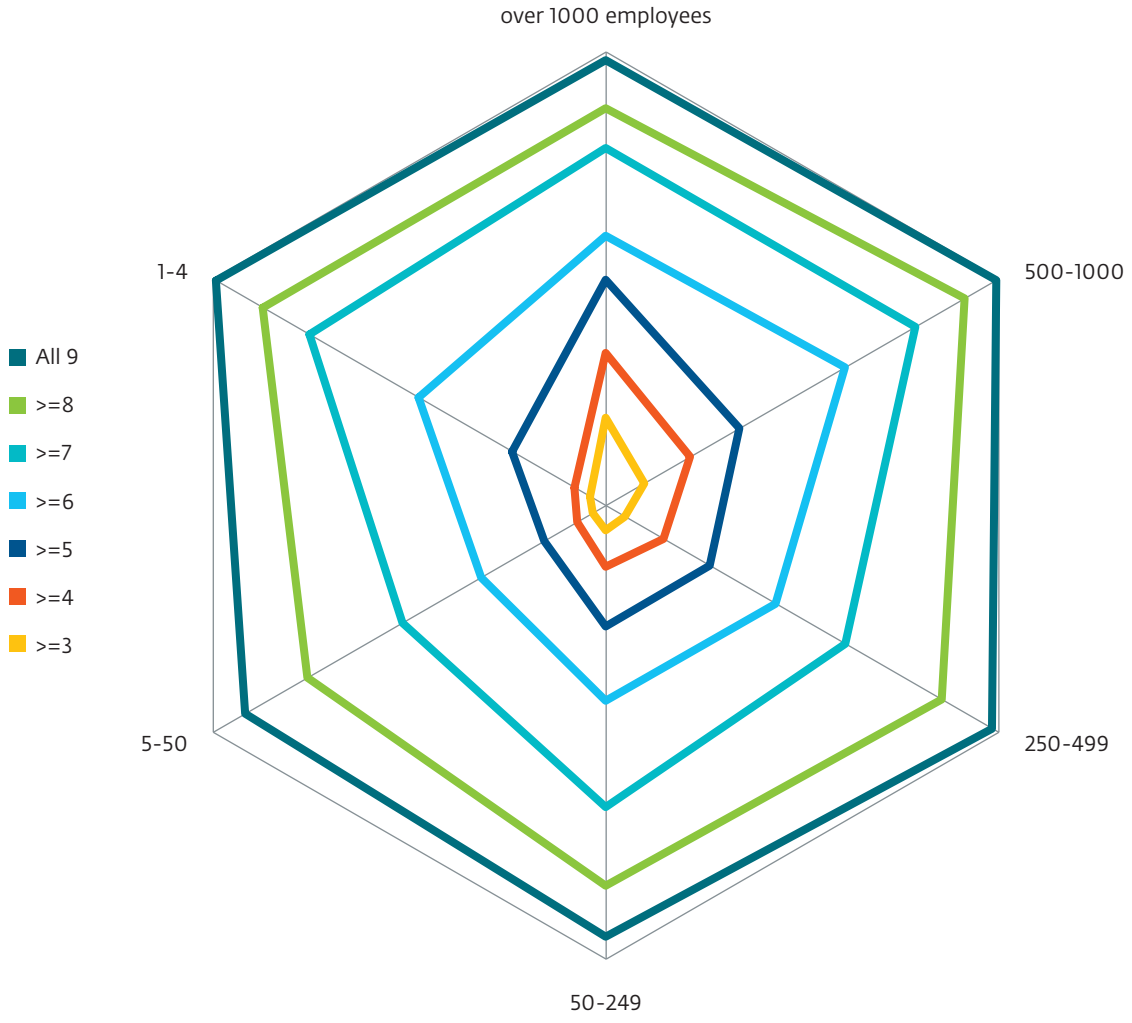
Over a **quarter (27%)** of the polled businesses still had, as of 2015, **no defined policy towards BYOD** in the workplace. With no centralized oversight, enforced update policy or mandatory use of security solutions, some of the loopholes for attackers might be left open.

When it comes to cyber security, (company) size matters

Out of the almost 1,700 companies ESET polled across the EMEA region, large enterprises seem to be more responsible when it comes to cyber security. With more vulnerabilities possibly open to the attackers, higher employee counts, and a wider scale of systems used, they opt for diversified protective measures more often than their smaller counterparts.

ESET's poll shows that **17% of enterprises** with over 1,000 employees **have all 9 monitored security measures** in place. This is almost double the rate compared to the **9%** adoption in firms with a headcount ranging from **500 to 1,000; small and medium-sized (SME) companies** fare even worse in the same comparison **(3-5%)**.

Number of implemented security solutions v. company headcount



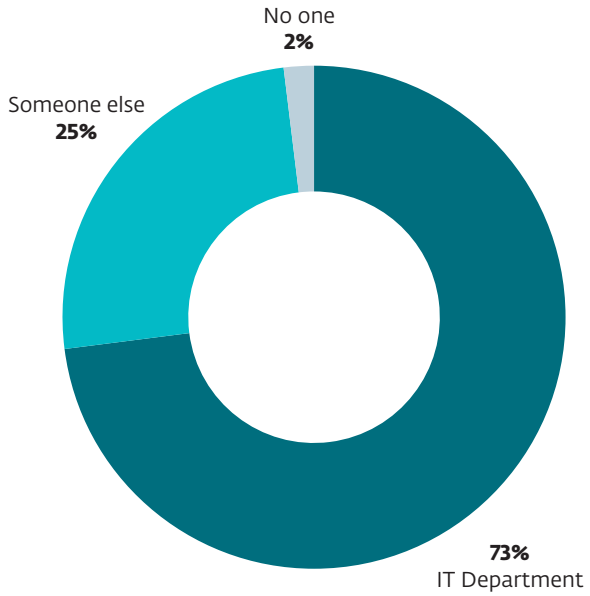
4) http://www.welivesecurity.com/2013/12/18/companies-have-heads-in-sand-about-security-threat-as-employees-sneak-mobile-devices-to-work-report-warns/

Who is responsible for cyber security?

Taking responsibility for cyber security in organizations seem to be a responsibility that falls mostly to **IT departments**. ESET's research shows that this is the case in almost three-quarters of the companies polled **(73%)**.

On the other hand, according to the responses, the remaining quarter **(25%)** have – at least partially – passed this task also to people in **managerial positions**. Only about 2% say they have **nobody specifically dedicated** to cyber security.

Who is responsible for IT security in your company?



The poll shows that a significant proportion of EMEA companies are still not investing in cyber security awareness activities for their employees. According to the respondents, **IT security training** was organized only by **37%** of EMEA firms, leaving many of them with a workforce lacking a proper knowledge of cyber threats.

From the managerial tools that can help to raise the level of protection, security policies are in place in a significant proportion of the EMEA companies polled. What raises eyebrows is the fact that less than one-third of them **(30%)** have a **system to classify information** that would allow them to identify the crucial pieces of data requiring higher level of protection.

An even smaller proportion **(23%)** of the firms in the poll reported having an **incident response plan** that defines actions to be taken in case of security breach, data leakage or other form of cyberattack.

(In)Sufficient IT security funds

Only **38%** of EMEA business respondents polled by ESET **consider the IT security budget of their company to be sufficient**.

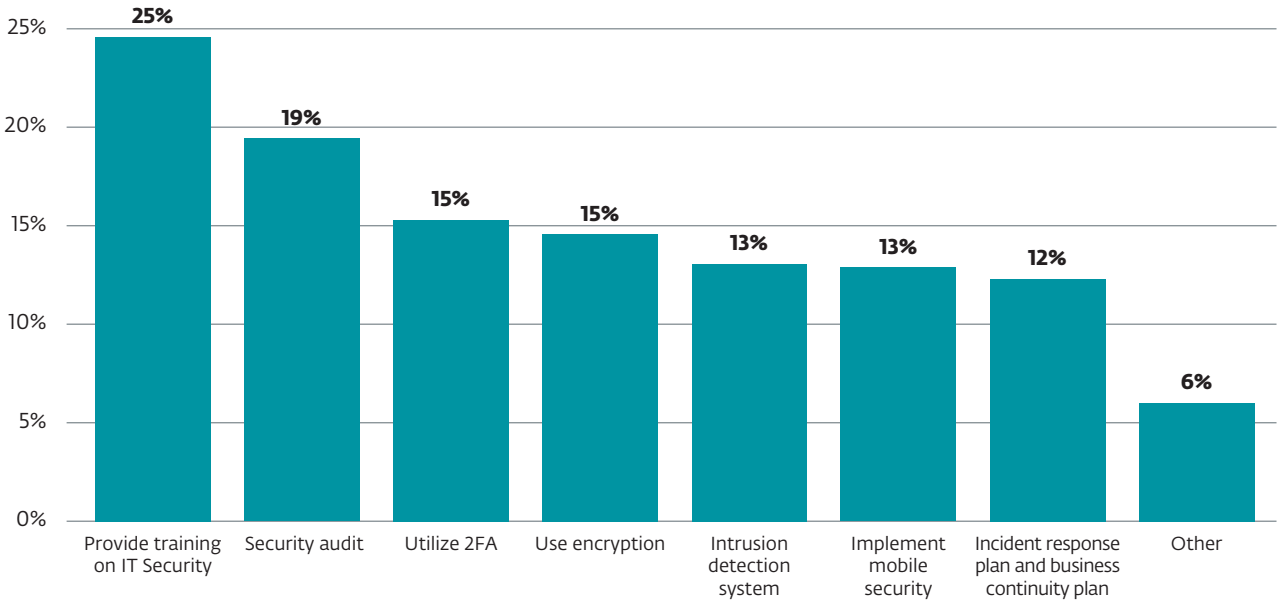
This leaves a lot of room for improvement, as more than 6 in 10 firms were unable to judge, or regard the funds allocated as insufficient.

> *"Only 38% of EMEA business respondents polled by ESET consider the IT security budget of their company to be sufficient."*

On the other hand, many of the respondents have a very clear idea of what they would do if they could spend more money on cyber security. The largest chunk **(25%)** of them would opt for **providing more cyber security training for employees**, followed by **19%** who would invest money into **security audits**.

Only about every seventh EMEA company **(15%)**, would utilize either **encryption** or **two factor authentication (2FA)**. **Mobile security** ranks lower on the interest list, even though BYOD seems to be relatively widespread in the region, with only **13%** of polled respondents saying they would secure portable devices if their budget was higher.

If you could spend more on IT security, what would you do?



Methodology

ESET, as a pioneer of antivirus protection, organizes and takes part in several regional and international security and technological conferences and public events, such as ESET Security Days, Mobile World Congress, IP Expo and many more.

This active role offers ESET the chance to meet and communicate with companies concerned about cyber security threats, discuss the possible impact on their businesses, and offer them solutions for their problems.

We should stress that this paper does not aspire to be a deep or exhaustive analysis of the current security situation in region. Its main goal is to give readers an insight into the cyber security issues that companies in the EMEA region are grappling with and identify some of the issues that might have gone unnoticed or unaddressed.

To create the Business Surveys 2015 report, we collected data from 10 EMEA countries (United Kingdom, Germany, Spain, Hungary, Slovakia, Lithuania, Greece, Netherland, Nigeria and Ghana) and one broader region (Middle East). The questionnaire focused on multiple issues, some of which are described above. We polled participants at regional and international security events.

The basic sample contained around 1,700 questionnaires, filled in by respondents occupying different positions in EMEA companies – ranging from employees in IT departments and their superiors, to C-level executives and company founders.

For the company size distribution, see the table below.

Company size	1-4	5-50	51-249	251-499	500-1,000	Over 1,000
	27	782	346	113	123	241


ENJOY SAFER
TECHNOLOGY™