

Top trends on IT Security Market

IT Security Conference, Sept 2009

Neli Vacheva,
Country Manager
IDC Bulgaria



IDC Market Coverage

Central & Eastern Europe, Middle East & Africa

Central and Eastern Europe

- Albania
- Austria
- Belarus
- Bosnia & Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Estonia
- Greece
- Hungary
- Kazakhstan
- Latvia
- Lithuania
- Macedonia
- Montenegro
- Poland
- Romania
- Russia
- Serbia
- Slovakia
- Slovenia
- Tajikistan
- Turkmenistan
- Ukraine
- Uzbekistan
- Rest of CEE



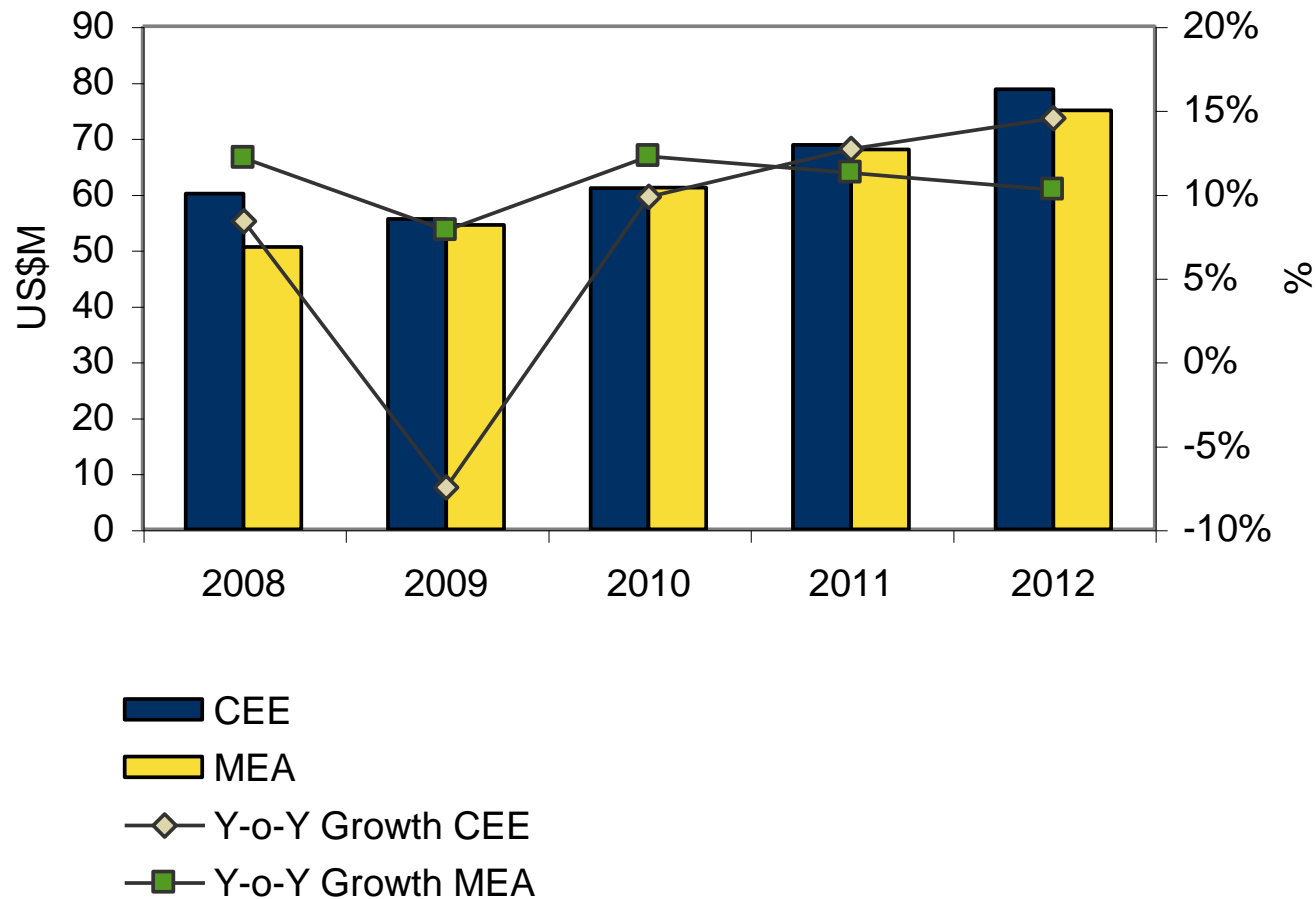
Middle East and Africa

- Turkey
- UAE
- Saudi Arabia
- Kuwait
- Qatar
- Oman
- Bahrain
- Lebanon
- Syria
- Iran
- Jordan
- Israel
- Rest of ME
- Egypt
- Morocco
- Algeria
- Tunisia
- Libya
- Ghana
- Kenya
- Uganda
- Nigeria
- Namibia
- Ivory Coast
- Ethiopia
- Tanzania
- Botswana
- South Africa
- Rest of Africa

IDC CEMA

- 120+ анализатора в 20 ключови страни от ЦИЕ и СИА
 - Регионален офис в Прага, Чехия
 - Проучвания на пазарите в 50 страни
- Изследователски регионални центрове: Core Central Europe, Russia/CIS, Adriatics, SEE, Middle East and Africa

CEMA IT Spending



Source: IDC Q4 2008 Worldwide Black Book

Organizations looking for ways to cut hardware costs and simplify IT management

Expanding mobility and search for productivity boost

Increased danger of Data Leakage – Incidental or voluntary

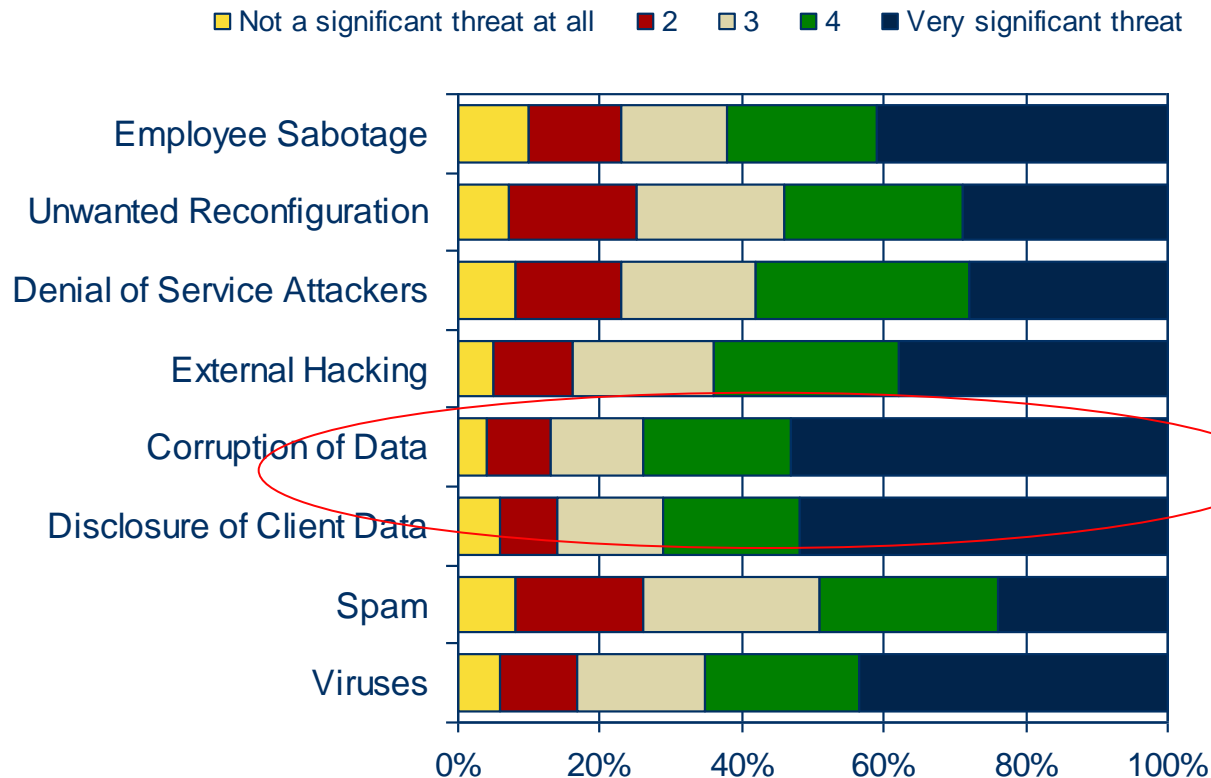
Fines for not meeting regulatory laws threaten existence of firms

Continued expansion of Web 2.0 causes more vulnerabilities

Protection of intellectual property becoming a priority

Green Initiatives

Top Threats in CEE

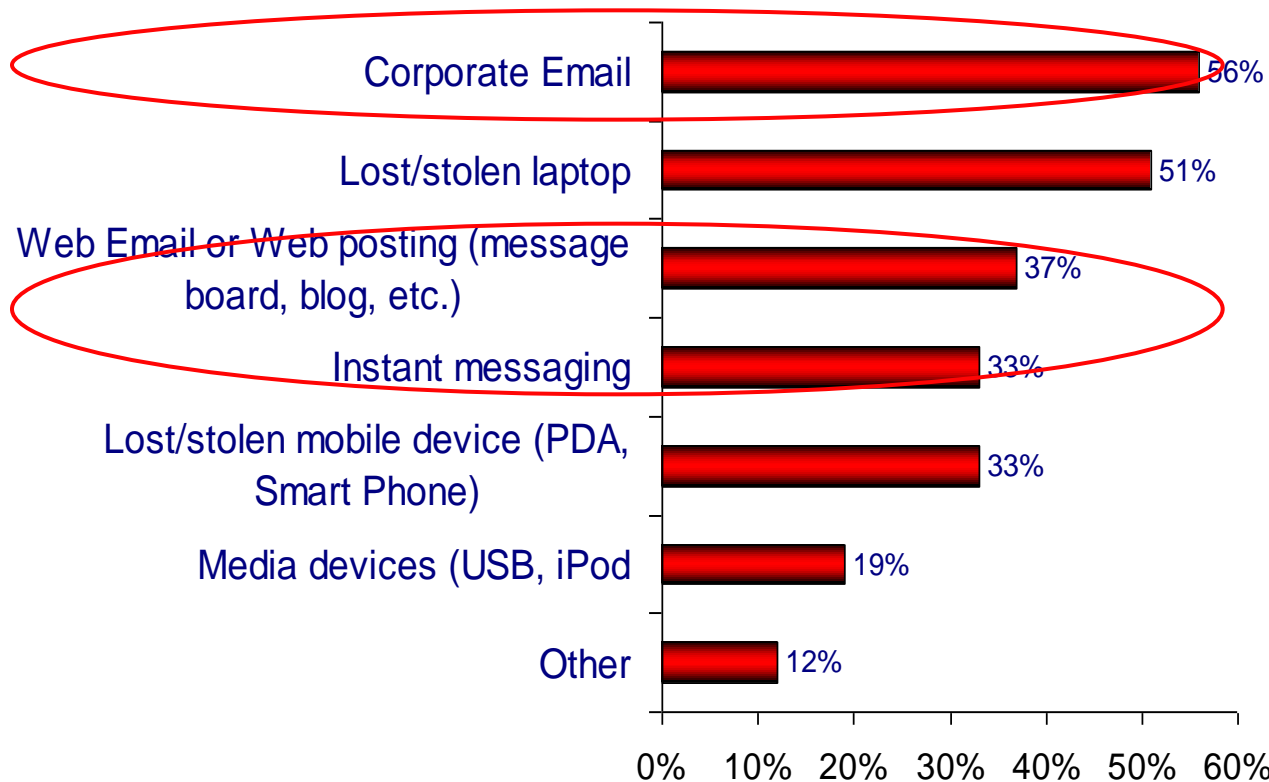


Q. Please rate the following threats in terms of their seriousness for your organization's network, data, and Internet security.

Source: IDC CEMA Security Roadshow 2008 Attendee Survey

How does the leaks of confidential information occur?

Base: 43 respondents (Among those who have experienced leaks of confidential information in the past 18 months) (Please check all that apply)



74% of the organizations believe, that monitoring e-mail is very important for DLP

More effective messaging security

Increased spending on e-mail security

bi-directional security

More-effective anti-spam solutions

E-mail encryption and data loss prevention

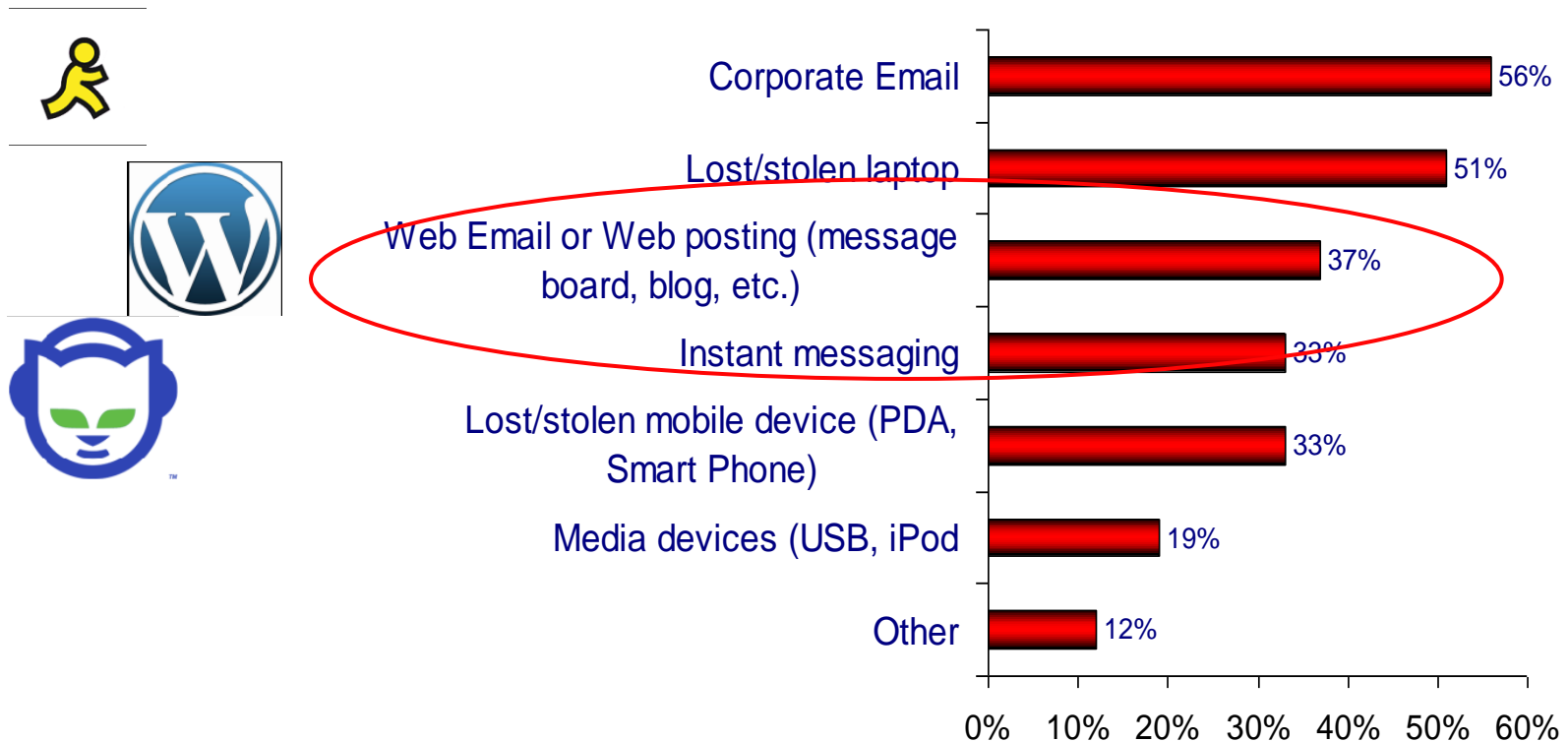
Adoption of virtual security appliances



***“The accidental provides
opportunity for the intentional.”***

Small finance

Web 2.0 Technologies Bring New Security Risks the past



74% of the organizations believe, that monitoring e-mail is very important for DLP

More than Anti-Virus

Similar to SMTP, AV is needed on HTTP channel but AV is not enough
Key is protection against botnets, malicious active content, XSS and various browser exploits.

More than URL Filtering

- URL filtering is required but it is not enough
- Key is Web 2.0 application control. Offering right access to right users for Web 2.0 (e.g., marketing can publish on Facebook, others can only view)

Data Loss Prevention

Ability to inspect outbound HTTP traffic is critical
Enforce DLP policy by applications or user groups (e.g., Source code or customer lists can't be sent via Webmail or IM).

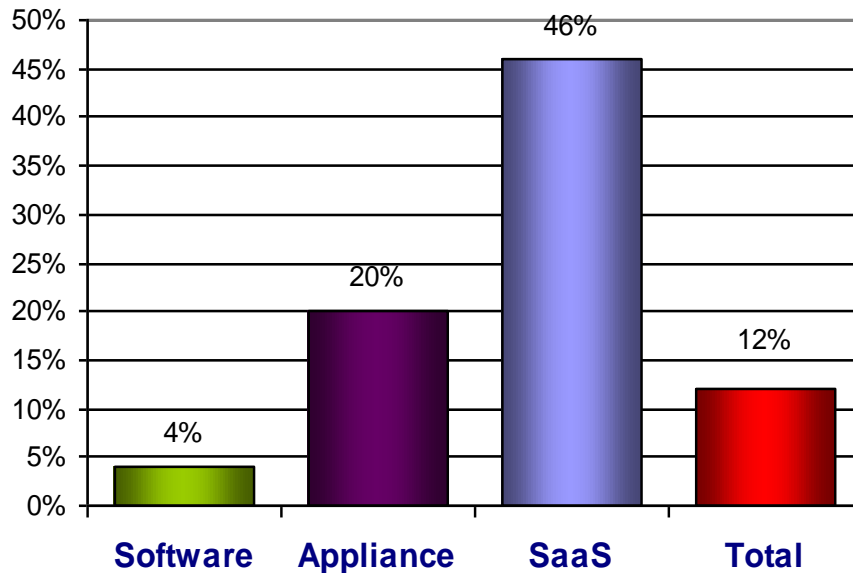
Logging & Reporting

Retain web logs for a longer period and access them on-demand
Ability to get flexible reporting by users, departments, applications and locations; Drill-down to transaction-level for detail.

Enterprise Readiness

Full redundancy & reliability
Integration with directory for user/group based policies
Ability to support mobile/roaming users without another desktop plug-in

SaaS Compound Annual Growth Rate (CAGR) 46%



Advantages of SaaS model adoption

- Cost – Opex than Capex
- Treat detection better, easier updates
- Easy of implementation and use
- Fewer IT resources
- Latency due to traffic rerouting
- Less control
- Environment Friendly

IT Security as a Service: Data Loss Prevention Solution, Case March 2009

prevents confidential information from leaving a customer's network, blocking the copying of any data in any external drives, electronic faxing or printing

Enable customers to locate their confidential data and conduct a pre-deployment risk assessment

DATA LOSS PREVENTION Solution

Endpoints policy push

network-based solution that: monitors and prevents data loss with comprehensive coverage,

DLP: email, instant messaging (IM), Web, Secure Web (HTTPS), FTP, peer to peer (P2P), and generic TCP

managed security services portal with security status information, alerts, and escalation reporting

Discovery capabilities

“Cloud Computing (“Cloud”) separates application and information resources from the underlying infrastructure and mechanisms used to deliver them with the addition of elastic scale and the utility model of allocation”

Source: Cloud Security Alliance

Cloud computing (SaaS, IaaS, PaaS)– IT Security Areas of focus

Challenges

- Who manages it
- Who owns it
- Where it's located
- Who has access to it
- How it's accessed

Changes in Security policy: does I have the same control over the applications and services?

Am I still secure and meeting the SLA

Compliance, may I prove it to auditors

How do I solve old security problems, like vulnerabilities, patch management, system integrity?

Source: Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance

- Organizations must accelerate their adoption of next generation security solutions, the cost of not doing so is increased malware infection, data leakage, and financial loss;
- New platform options, such as SaaS, should be explored as part of this adoption and organizations should find vendors which provide next generation technologies.
- Corporate DMZ is cluttered with security point appliances (appliance fatigue). Organizations using multiple point appliances should take this opportunity to consolidate in order to reduce administrative and support costs.
- In-the-cloud security should include careful Risk assessment, if done right, can consolidate point products, simplify them and reduce cost
- Latency is the hardest problem to solve for in-the-cloud security service. Distributed, multi-tenant architecture is key to solving it.



Can You Economize on Security and How?

Yes you can:

- Cloud computing (SaaS) and security as a service
- Unified security mgmt
- Appliances
- Review technology stack
- Standardize the infrastructure
- Implement policy, follow it
- Open source (watch the overhead cost!)



Thank You 



Neli Vacheva

Tel: + 359 2 9693056
nvacheva@idc.com

Country Manager
IDC Bulgaria

IDC Bulgaria
Dragan Tzankov Blvd, 36
1040 Sofia
Bulgaria

www.idc-cema.com
www.idc.com