Cisco 2011 Annual Security Report

Global Security Threats and Trends

Cisco 2011 Annual Security Report
Summary / Key Takeaways

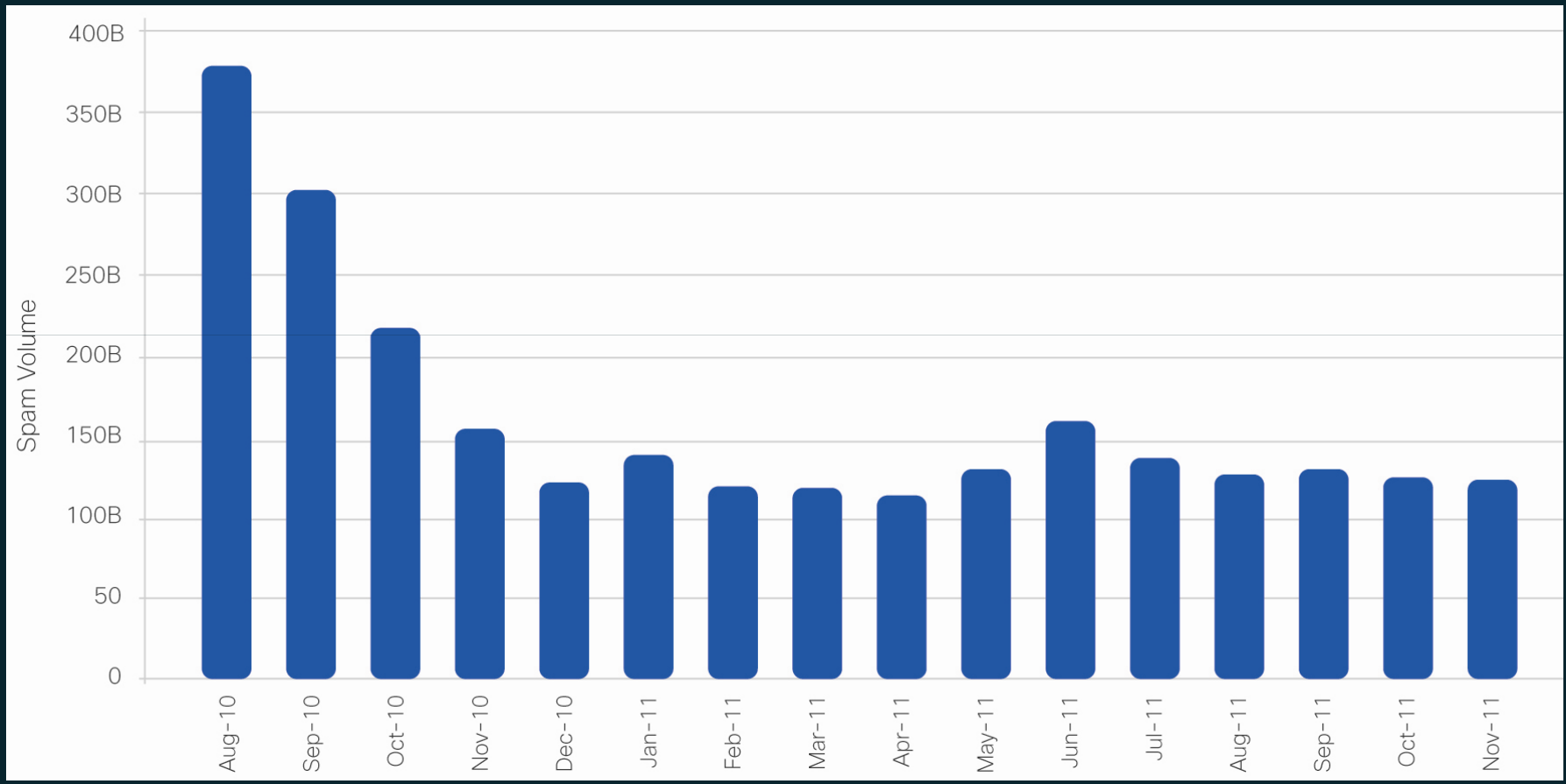
Dramatic decline in spam volume

- From 379 bn messages daily (Aug 2010) to 124 bn messages daily (Nov 2011)

Widespread attacks replaced by targeted attacks

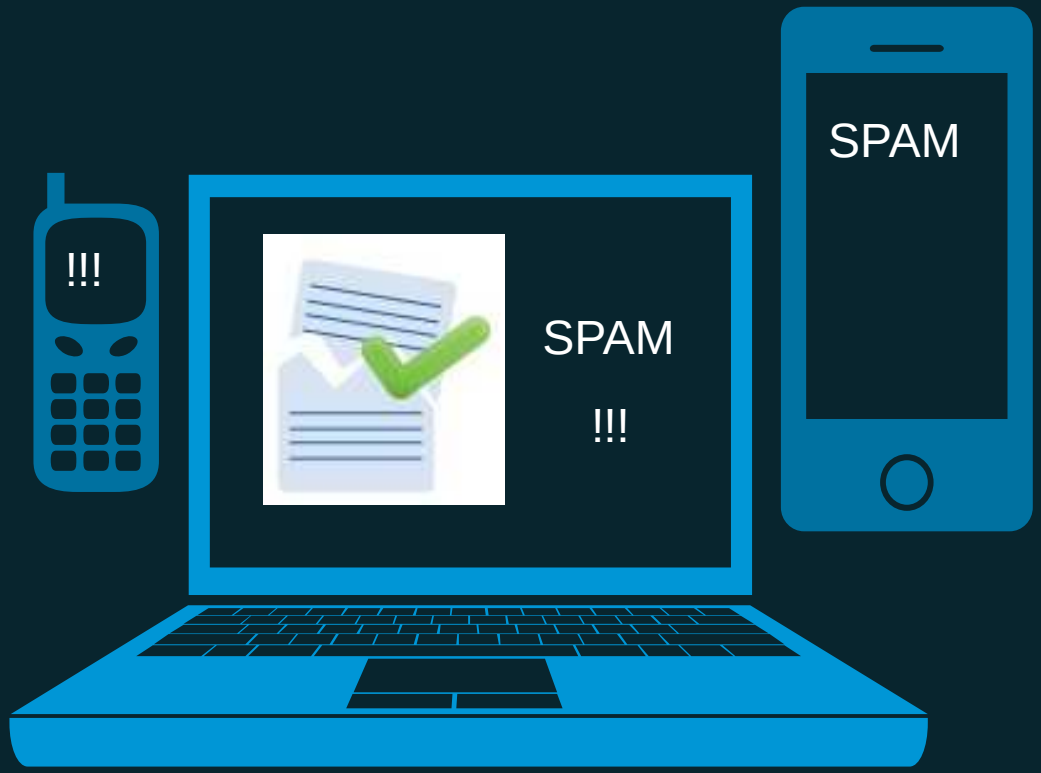
Future workers tend to ignore online threats

Global spam volumes



Source: Cisco SIO

Spam trends in Romania



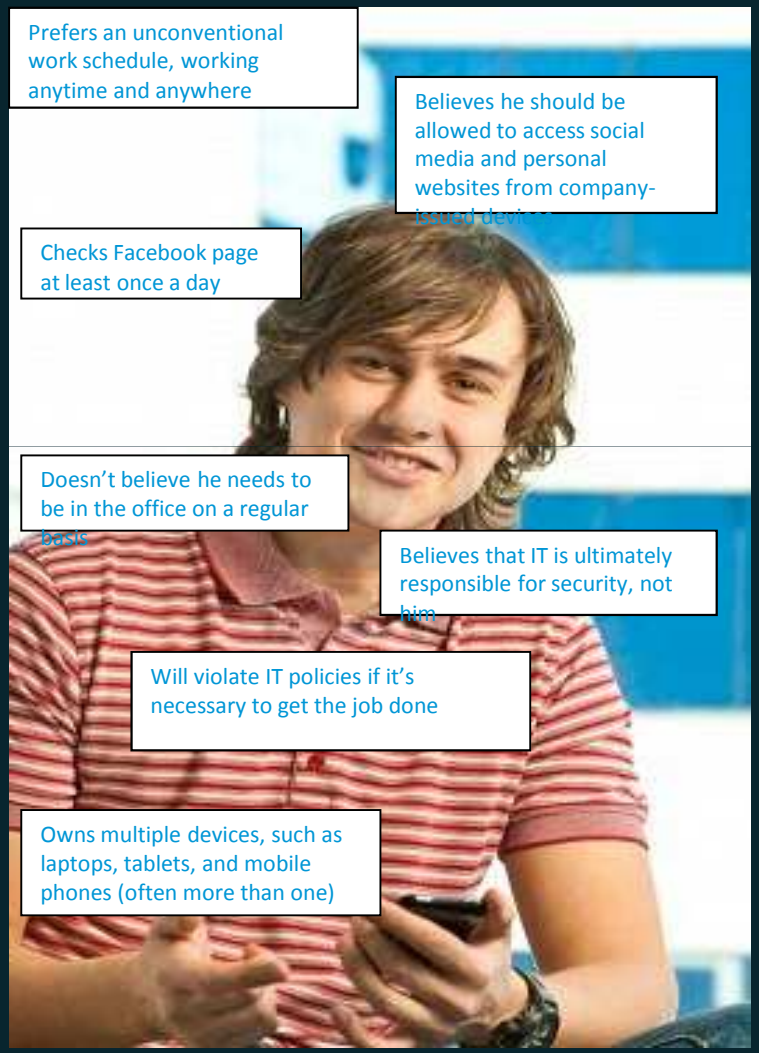
Spam level changes 2010-2011

Bulgaria: 79% drop
Germany: 93% drop
Hungary: 91% drop
Poland: 85% drop

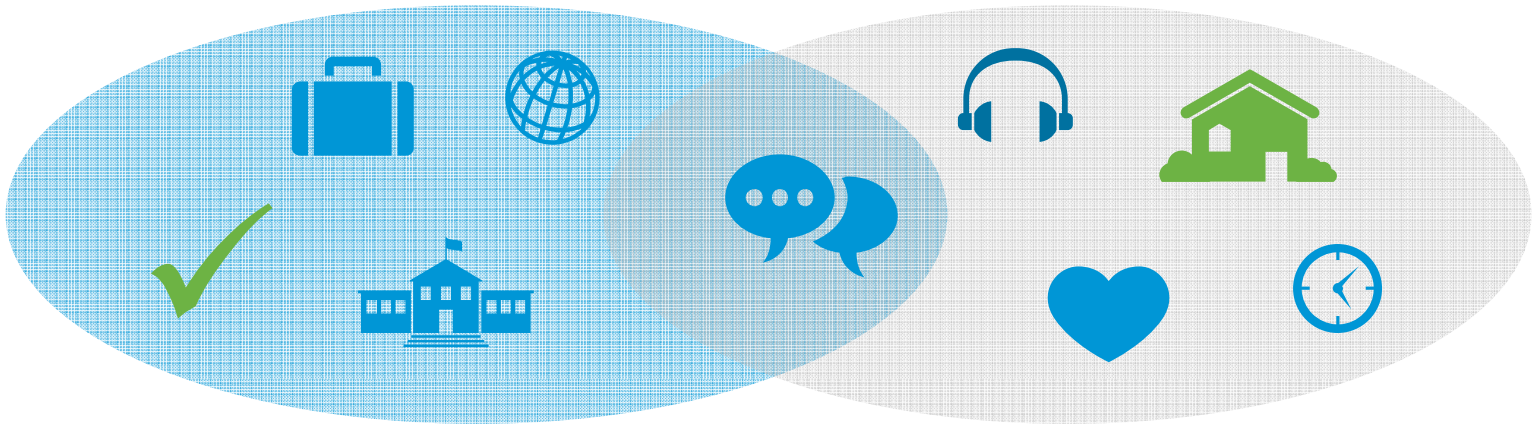
- Spam volumes in 2011 dropped 82% vs. 2010
- % of global spam originating from Romania in 2011: 2,56%

The Cisco Cybercrime Return on Investment Matrix: winners and loosers in 2012

Future workers and online threats: the anytime, anywhere young worker

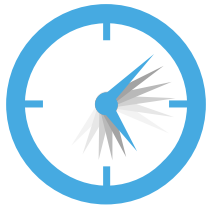


Cisco Connected World Technology Report Summary of Key Findings



- ‘Millennials’ have grown up with the Internet and have an increasingly on-demand lifestyle that mixes personal and business activity in the workplace
- The majority of employees believes it’s the company’s responsibility to protect information and devices – not their own
- College students and young professionals are taking extreme measures to access the Internet, even if it compromises their company or their own protection
- The ability to ensure policy compliance involving social media, devices, and remote access is testing the limits of traditional corporate cultures and placing greater pressure on recruiters, hiring managers, and IT departments to allow more flexibility
- IT teams continue to need to address their mobile device policies as the tablet wave increases

Adhering to IT policies



70% (7 of 10)

OF EMPLOYEES

ADMITTED TO BREAKING POLICY WITH VARYING REGULARITY

61% (> 3 of 5)

OF EMPLOYEES

BELIEVE THEY ARE NOT RESPONSIBLE FOR PROTECTING INFORMATION ON DEVICES

80% (4 of 5)

OF EMPLOYEES

SAID THEIR COMPANY'S **IT** POLICY ON SOCIAL MEDIA AND DEVICE USAGE POLICY WAS EITHER OUTDATED — OR WEREN'T SURE IF SUCH A POLICY EXISTED AT ALL

Adhering to IT policies…or not

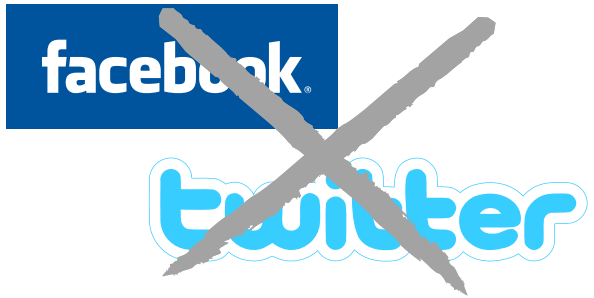
REASONS EMPLOYEES BREAK **IT** POLICIES

- **22%** CITE THE NEED TO ACCESS UNAUTHORIZED PROGRAMS AND APPLICATIONS TO GET THEIR JOB DONE
- **19%** ADMITTED THE POLICIES ARE NOT ENFORCED
- **18%** DON'T HAVE TIME TO THINK ABOUT POLICIES WHEN THEY ARE WORKING
- **16%** SAID IT'S NOT CONVENIENT
- **15%** FORGET
- **14%** DO IT WHEN THEIR BOSSES AREN'T WATCHING THEM

IT Policies – Mobile Devices and Social Media

1 in 10

EMPLOYEES SAID THEIR IT POLICIES PROHIBIT THE USE OF IPADS AND TABLETS



3 of 10

SAID SOCIAL NETWORKING SITES LIKE FACEBOOK, TWITTER, AND YOUTUBE WERE PROHIBITED BY THEIR COMPANIES

Borrowing Eggs, Sugar…and Wireless Internet?

1 of 4 (23%) HAVE ASKED THEIR NEIGHBORS IF THEY CAN USE THEIR COMPUTER OR FOR INTERNET ACCESS

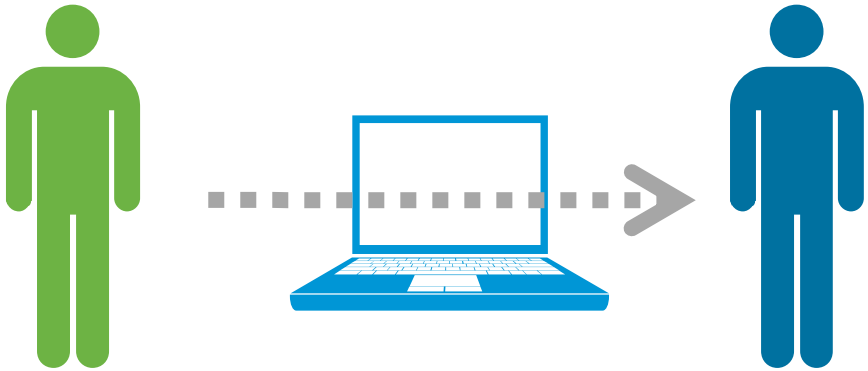
1 of 5 (19%) HAVE ACCESSED THEIR NEIGHBOR'S WIRELESS CONNECTION WITHOUT TELLING THEM

ADMITTED STANDING OUTSIDE OF RETAIL OUTLETS TO USE FREE WIRELESS CONNECTIONS

1 of 10 (9%) HAVE ASKED A STRANGER TO USE THEIR MOBILE PHONE

2 of 3 (64%) **HAVE DONE AT LEAST ONE OF THESE ACTIONS**

Risky Business: Unsupervised Computer Usage



56% (>1 of 2)

OF EMPLOYEES

SAID THEY HAVE ALLOWED OTHERS TO USE THEIR COMPUTERS WITHOUT SUPERVISION – FAMILY, FRIENDS, BUSINESS PARTNERS, COWORKERS, AND EVEN PEOPLE THEY DO NOT KNOW

86% (>4 of 5)

COLLEGE STUDENTS

SAID THEY HAVE ALLOWED OTHERS TO USE THEIR COMPUTER UNSUPERVISED

16% (>1 of 10)

COLLEGE STUDENTS

ADMITTED LEAVING PERSONAL BELONGINGS AND DEVICES UNATTENDED IN PUBLIC

Risky Behavior's Impact on Identity Theft Rates

1 of 3 COLLEGE STUDENTS

- DO NOT MIND SHARING PERSONAL INFORMATION ONLINE
- BELIEVE PRIVACY BOUNDARIES ARE LOOSENING
- DO NOT THINK ABOUT PRIVACY

ANY WONDER?

1 of 4 ONE IN FOUR EXPERIENCE IDENTITY THEFT BEFORE THE AGE OF 30

AND

2 of 5 COLLEGE STUDENTS

KNOW OF FRIENDS OR FAMILY MEMBERS WHO HAVE EXPERIENCED IDENTITY THEFT

Summary

- Students and young professionals believe their generation is at least moderately concerned about Internet security threats – although don't always use common sense to protect themselves or company assets
- In a sign that the Internet is so critical in people's lives – whether as important as food, air, and water or not – a striking number of employees would go to great lengths to access the Internet
- These findings beg the questions:
  - *Will the next generation of workers be even more demanding of Internet access, no matter what the cost or condition?*
  - *How will this impact the rate of identity theft and corporate data loss globally?*

Cisco Annual Security Report
2012 Outlook

Continued trend of targeted attacks replacing mass attacks

Hacktivism

Attacks on critical infrastructure systems / SCADA

3 business trends with security implications

Remote access

Bring Your Own Device

Cloud-based file-sharing

Identity management, Device management, DLP policies

Recommendations

1. **Assess the totality of your network.**
2. **Re-evaluate your acceptable use policy and business code of conduct.**
3. **Determine what data *must* be protected.**
4. **Know where your data is and understand how (and if) it is being secured.**
5. **Assess user education practices.**
6. **Use egress monitoring.**
7. **Prepare for the inevitability of BYOD.**
8. **Create an incident response plan.**
9. **Implement security measures to help compensate for lack of control over social networks.**
10. **Monitor the dynamic risk landscape and keep users informed.**

Thank you.