

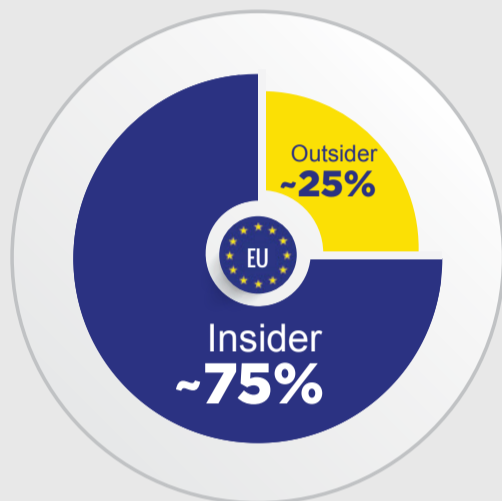
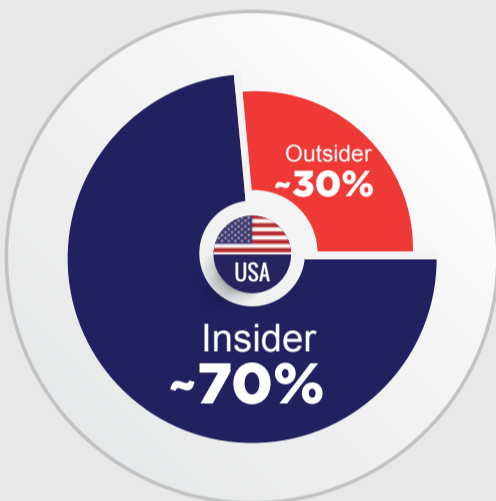


# Balabit CSI Report



## Black Hat Survey Results: Know Your Enemy from the **TOP 10** Most Popular Hacking Methods

Balabit conducted one of its recent surveys among 494 IT security professionals at two major events in 2015: Black Hat USA Conference in Las Vegas and Black Hat Europe Conference in Amsterdam. On the one hand, the survey shows whether IT professionals consider their own employees or the outsider attacks more risky. On the other hand, it aims to highlight the TOP 10 most popular hacking methods helping organizations to clearly see which methods or vulnerabilities attackers are using the most - or taking advantage of - when they want to get sensitive data in the shortest time.



### Insider or outsider? Not that obvious

Balabit surveyed whether IT professionals consider the outsider or insider threats more risky - noted that those attacks that are started from outside by attackers primarily targeting insiders' privileged user accounts (so would never be successful without insider help of insider user accounts misuse), belong to the insider category. Although, respondents said that they are still afraid of "hackers" breaking into their IT network, the results highlight a good point to an efficient defense strategy: in the USA 70% of those surveyed said that insiders are more risky, and only 30% stated that outsiders pose higher risk. However, this ratio is even more imbalanced in the EU: 75% of respondents consider insiders more risky as opposed to outsider risk with 25%.

## Top 10 Hacking Methods

The survey result unveils the list of the TOP 10 most popular hacking methods clearly highlighting the need that organizations must know what is happening in their IT network in real time. This can only be achieved by complementing the existing control type of security tools with continuous monitoring that alerts and blocks harmful incidents in case of suspicious activities, and highlights anomalies that are worth investigating.



	USA	EU	
1	81%	83%	<b>SOCIAL ENGINEERING</b> (e.g. phishing)
2	62%	63%	<b>COMPROMISED ACCOUNTS</b> (e.g. weak passwords)
3	51%	54%	<b>WEB-BASED ATTACKS</b> (e.g. SQL/command injection)
4	33%	43%	<b>CLIENT SIDE ATTACKS</b> (e.g. against doc readers, web browsers)
5	23%	17%	<b>EXPLOIT AGAINST POPULAR SERVER UPDATES</b> (e.g. OpenSSL, Heartbleed)
6	21%	16%	<b>UNMANAGED PERSONAL DEVICES</b> (e.g. lack of BYOD policy)
7	15%	13%	<b>PHYSICAL INTRUSION</b>
8	11%	10%	<b>SHADOW IT</b> (e.g. users' personal cloud-based services for business purposes)
9	9%	10%	<b>MANAGING THIRD PARTY SERVICE PROVIDERS</b> (e.g. outsourced infrastructure)
10	6%	6%	<b>TAKE ADVANTAGE OF GETTING DATA PUT TO THE CLOUD</b> (e.g. IAAS, PAAS)

### About the survey

Balabit, a leading provider of contextual security technologies and Silent Signal, a leading technology provider of state of the art ethical hacking services, jointly organized the eCSI Hacker Playground, a global online hacker competition, specially designed for the Black Hat USA 2015 conference in Las Vegas. The survey about the TOP 10 Most Popular Hacking Methods was conducted amongst 494 participants of the Black Hat USA conference in Las Vegas and months later at the Black Hat Europe in Amsterdam, in 2015. The Black Hat series gathers a wide range of IT security practitioners from IT Specialists, Security Analysts, Risk Managers, Security Architects/Engineers, Penetration Testers, Security Software Developers, Cryptographers, Programmers, Government Employees to Security Executives and Business Developers.