radware

CYBER-SECURITY PERCEPTIONS AND REALITIES

A VIEW FROM THE C-SUITE

High-profile assaults have elevated cyber-attacks to the front pages and onto the desks of C-suite executives. How are leaders responding to this new wave of botnets and malicious malware? Radware surveyed over 200 IT executives in the U.S. and Europe to find out.

AUTOMATION

Takes a Seat in the Boardroom

38%

38% foresee machine learning and AI as the wave of the not-so-distant future.

> **"Within two years, automated security systems – such as machine learning and artificial intelligence will be the primary resources to maintain cyber security."**

CYBER SECURITY

Remains Top of Mind

80% of executives affirm security is now a board-level concern.

80%

PRIVACY OR PROFIT?

Executives Support Greater Government Intervention

79%

Government should do more to protect consumers' personal information – even if it adversely affects day-to-day operations – according to **79%** of respondents.

MALWARE & BOTS

and Ransomeware, Oh My!

60% of executives say these three attack types would be most detrimental to their organizations.

60%

IN-HOUSE SECURITY

Management is Preferred

Globally, **54%** of executives prefer to manage cyber-security internally.

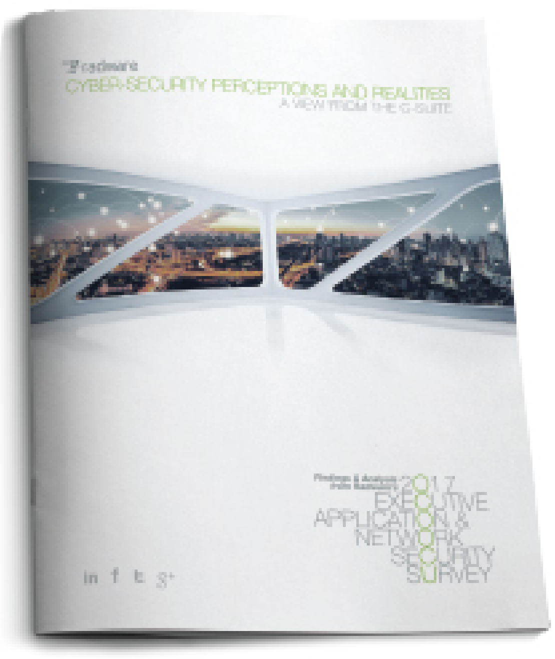
54%

HACKERS:

To Hire or Not to Hire

European leadership is more likely to hire ex-hackers than their American counterparts, **58% versus 27%**.

58% VS. 27%



How do you mitigate these threats and put company stakeholders at ease? The key is adopting the right approach.

DOWNLOAD THE *2017 EXECUTIVE APPLICATION & NETWORK SECURITY REPORT* TO LEARN HOW.

https://www.radware.com/c-suite-security-report-2017/

www.radware.com