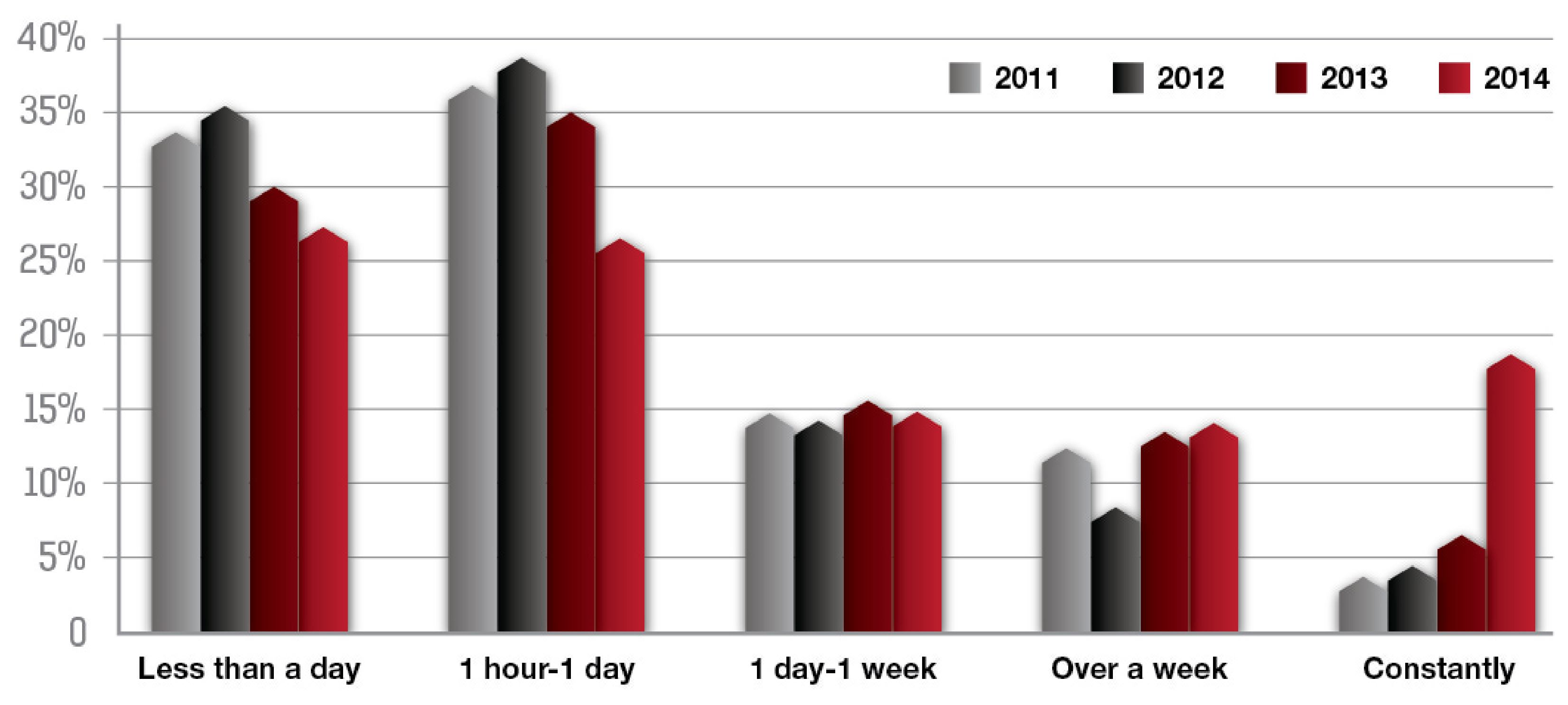
What's Keeping Us Up At Night?

2014 was a watershed year for the security industry. Cyber-attacks reached a tipping point in terms of quantity, length, complexity and targets. Even organizations with by-the-book security programs can be caught off guard.

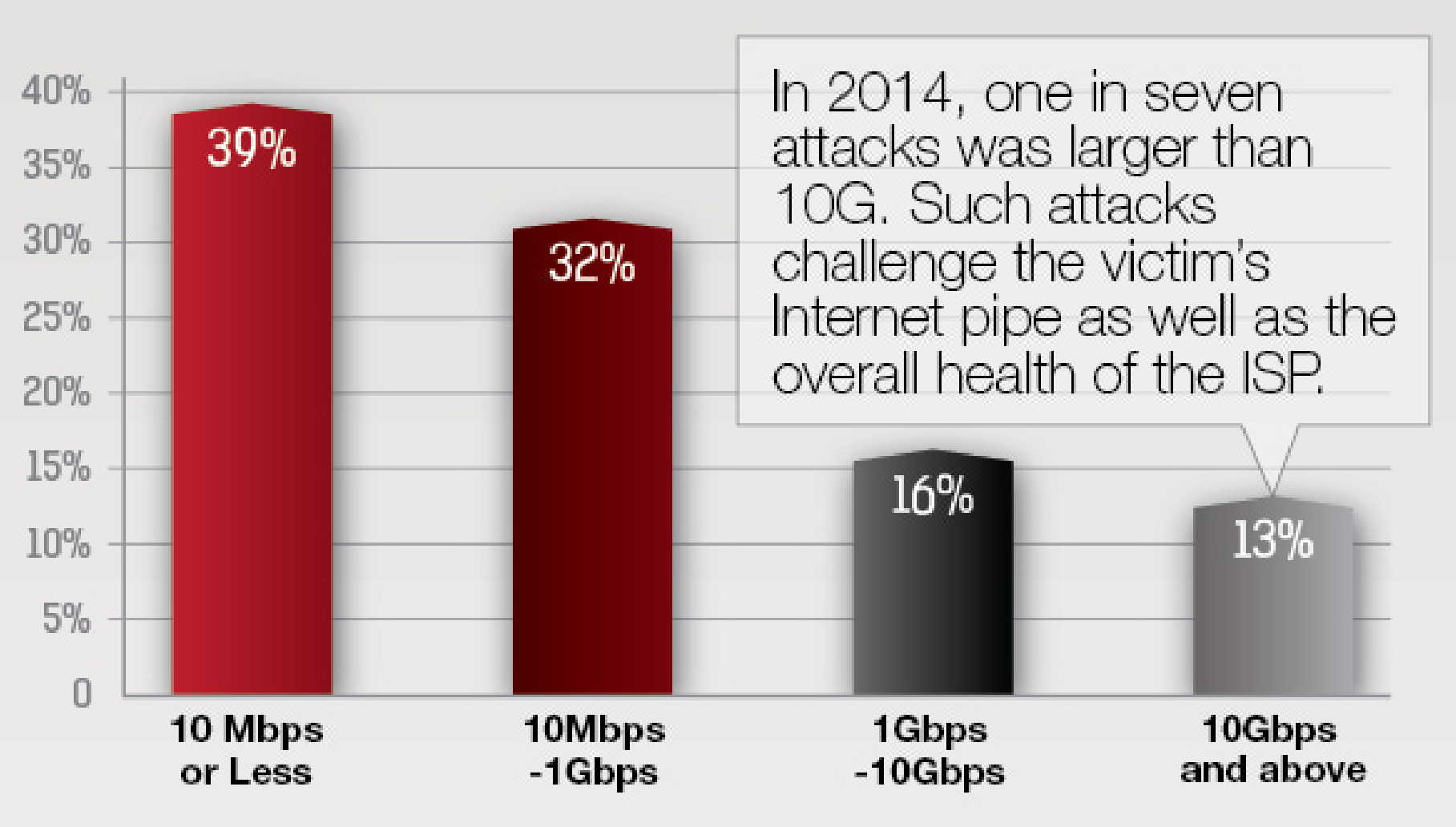
Constant Attacks are on the Rise

Attacks are evolving to become longer, larger and more sophisticated. Organizations reported week-long and month-long attacks in previous years–but never more than 6% reported experiencing constant attacks. This changed in 2014 when **19%** of the **major attacks** reported were considered **"constant"** by the targeted organization. **52%** of respondents felt they could only **fight** a campaign for **a day or less**.

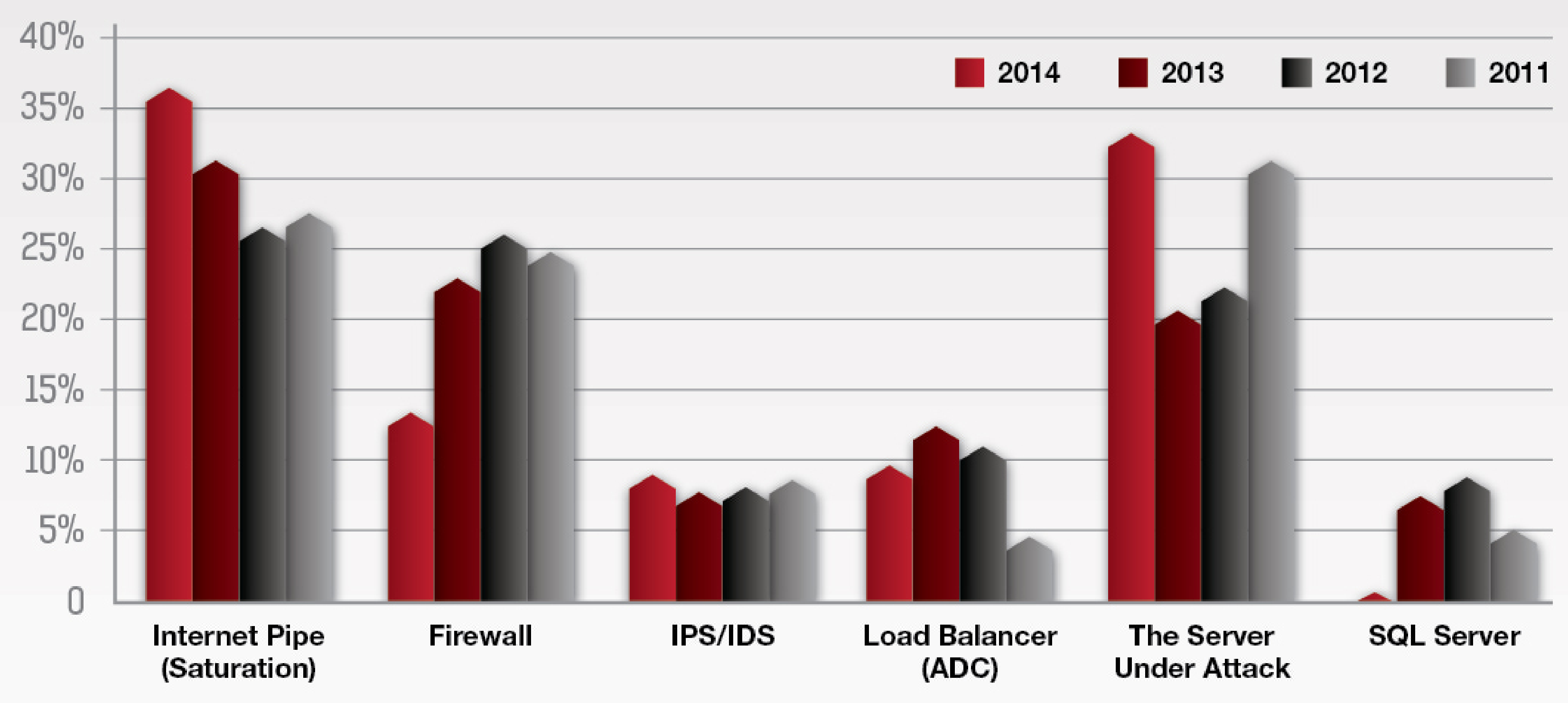


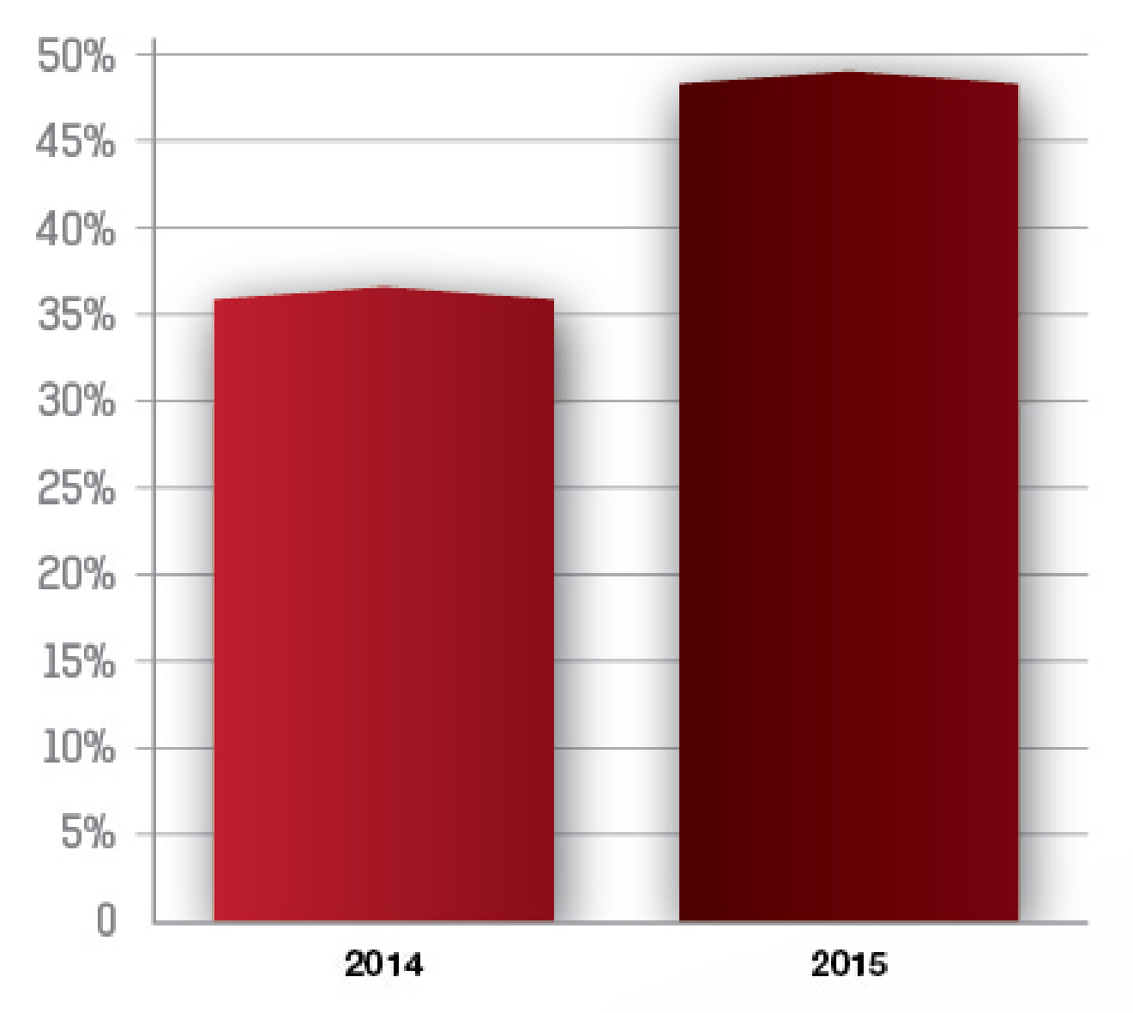
New Points of Failure in DDoS Attacks

The **Internet pipe** has been identified as the **number-one failure** point in 2014 and **reflective attacks** represent 2014's single **largest DDoS "headache."**



In 2014, one in seven attacks was larger than 10G. Such attacks challenge the victim's Internet pipe as well as the overall health of the ISP.





Hybrid Solutions Are Gaining Ground

More than **a third** of respondents have employed **hybrid solutions** to help gain ground against attacks, combining on-premise equipment with cloud solutions. Nearly **half** suggest that they will employ a **hybrid solution** by **2015**.

Information Security Has Three Incredibly Disruptive and Immutable Macro Trends

Mitigation techniques are being challenged with the emergence of **three** disruptive macro IT trends. Organizations that ignore or resist these trends, risk becoming obsolete.

1. Great Cloud Migration Continues. Enterprise IT Dissolves
2. Internet of Internet of Things (IoT) Brings an End to Controlled Endpoints and Introduces Incredible New Threats
3. The Software-Defined Network – disruptive, promising or both?

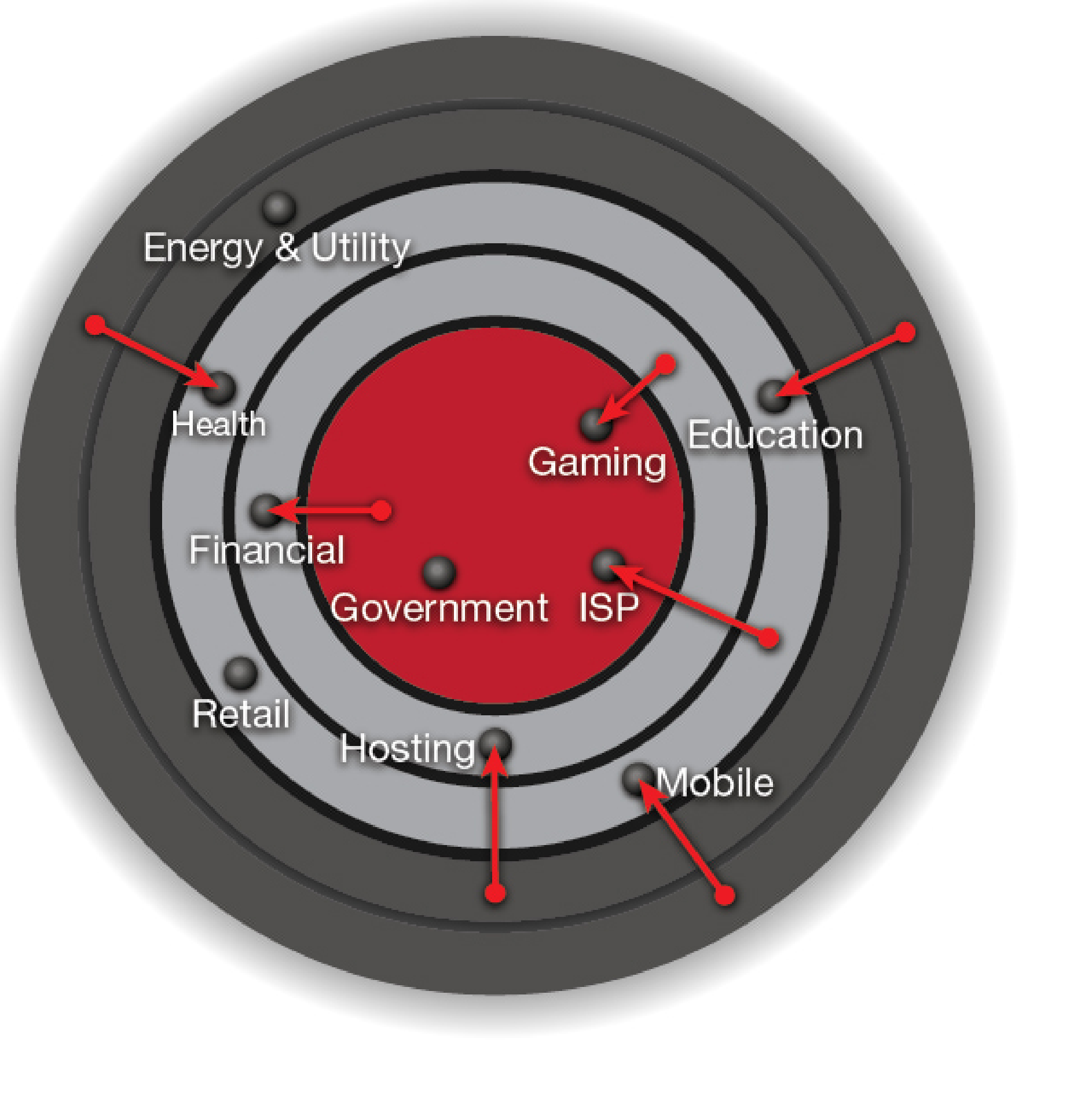
Losing Sleep in the C-Suite

As both **reputation loss** and **revenue loss from** a cyber-attack are **major concerns** for cyber-security **executives**, it's no surprise that nearly **three-quarters** of **executives** told us that security threats are now a **CEO or board-level concern**.

Cyber Attack Ring of Fire

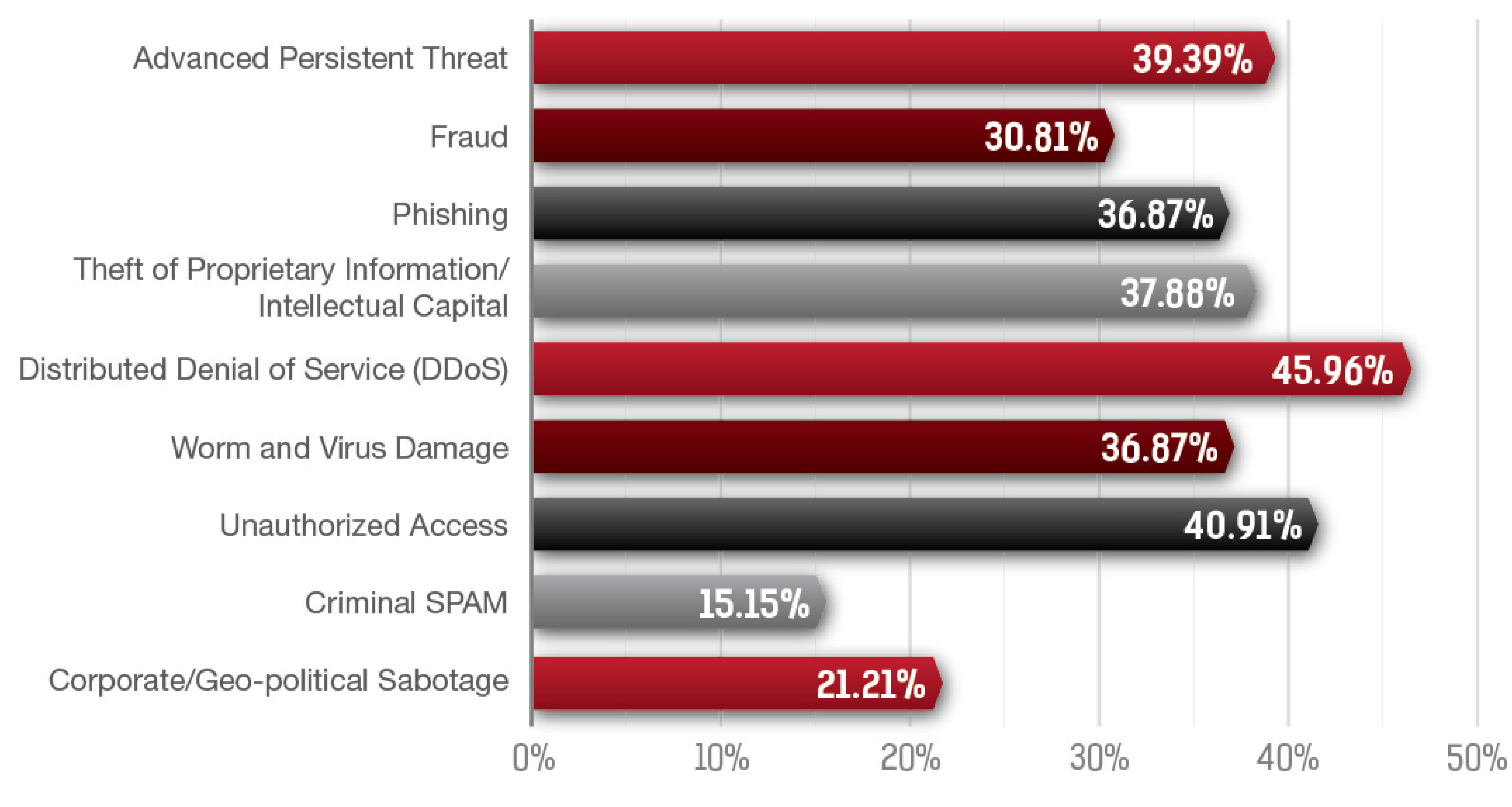
Risk is high or on the rise for some targets such as Gaming, Healthcare, Mobile, Hosting & ISP, Education, Financial and Government. As companies move toward the center susceptibility to cyber-attack grows, creating a security gap.

● 2014 → Change from 2013



The Most Threatening Threats

We asked which type of cyber-attack would cause the greatest harm to respondents' organizations. Although DDoS was the most-cited threat type, its lead is narrow. All of the threat types are fairly well represented—suggesting that the threat landscape varies depending on each organization's industry and business concerns.



What Can You Do?

When planning cyber-attack defense, be mindful of the C.H.E.W. threats (Cybercrime, Hacktivism, Espionage and Cyber War), be demanding of vendors and always consider the following tenets:

- **Cyber-Attack Defense = Attack Detection + Attack Mitigation.** Success hinges on both the quality and time of detection and mitigation.
- **Timing is everything.** Look at time to mitigate as a key success factor and ensure that the solution deployed provides the shortest time to mitigate.
- **Fill in the holes.** DDoS mitigation solutions need to offer wide attack coverage that can detect multi-vector attacks that hit different layers of the infrastructure.
- **Use multiple layers.** Resolve the issues of single-point solutions with cloud-based protection that blocks volumetric attacks plus an on-premise solution that blocks all other, non-volumetric attacks.
- **Mitigate SSL attacks.** SSL attacks will remain a major threat in 2015. Look for SSL-based DoS/DDoS mitigation solutions with a deployment that does not affect legitimate traffic performance
- **Look for a single point of contact.** In the event of an attack, it's crucial to have a single point of contact that can help divert Internet traffic and deploy mitigation solutions.

Download 2014-2015 Global Application & Network Security Report
http://www.radware.com/ert-report-2014/

radware ert

About Radware's ERT

The Emergency Response Team (ERT) has extensive experience handling attacks 'in the wild' as they occur. The findings in the report are a compilation of their front-line insights and formal surveys of worldwide security professionals on the state of cyber security.

radware
www.radware.com