



 radware

# Global Application & Network Security Report 2014-2015



- 01 Executive Summary
  - Cyber-Attacks Proving Tough to C.H.E.W.
  - Most Important Findings
- 02 Methodology and Sources
  - Security Industry Survey
  - Security Executive Survey
  - Emergency Response Team (ERT) Case Studies
- 03 Cyber-Attack Ring of Fire
  - Industries at High Likelihood for Attacks
  - Industries at Medium Likelihood for Attacks
  - Industries at Low Likelihood for Attacks
- 04 Business Concerns of Cyber-Attacks
  - The Great Unknown - Attack Motivation
  - The Most Threatening Threats
  - Most Pressing Concerns
  - Budgeting and Planning
- 05 Attack Vector Landscape
  - Application vs. Network Attacks
  - Multi-Vector Attacks Become 'Standard' in 2014
  - Attack Strength and Duration Increase
  - Attack Size: Does It Matter?
- 06 Notable Attack Vectors
  - Headless Browsers and DDoS - Attacks Become More Sophisticated
  - Mixed Attacks Are on the Rise
  - Points of Failure
  - Reflected Amplified Floods Remain a Key Challenge
- 07 Three Incredibly Disruptive and Immutable Macro-Trends in Information Security
  - Great Cloud Migration Continues. Enterprise IT Dissolves
  - Internet of Things (IoT) Brings an End to Controlled Endpoints and Introduces Incredible New Threats
  - The Software-Defined Network Is Changing the Rules of the Game
- 08 Case Studies
  - Anyone is a Target: DoS Attack Case Analysis on Boston Children's Hospital
  - Pay Up or Else: IT Infrastructure Solutions Provider Helps Customers Navigate Range of Network Attacks
- 09 Executive Insights—From the Corner Office
  - Industry-Specific Risks
  - Looking Back
  - Trendy—and Risky?
  - Losing Sleep: What's Keeping Executives Up at Night?
  - Looking Ahead
- 10 Cyber-Attack Protection Best Practices
  - Recap: C.H.E.W. – Motivation, Capability & Intent
  - Cyber-Attack Defense = Attack Detection + Attack Mitigation
  - How to Evaluate a Vendor for DDoS & Cyber-Attack Mitigation
- 11 Summary—The Fearful Five
- 12 Respondent Profile
- 13 Credits
  - Authors
  - Advisory Board
  - About the Authors





## 01

### Cyber-Attacks Proving Tough to C.H.E.W.

In August 2013, former U.S. Assistant Defense Secretary for Homeland Defense & Americas' Security Affairs, Dr. Paul Stockton, participated in a panel discussion about cyber-security challenges facing utilities—including some of the vulnerabilities within the U.S. electric grid system. Dr. Stockton asserted that if a successful computer network hack were to bring down the grid for a significant period, critical lifeline infrastructure would fail. Even temporary loss of the nation's hospital, transportation, food or pharmaceutical distribution infrastructure could threaten public health and safety.

This underscores the importance of understanding the preparedness not only of our energy sources but also of every player within a nation's critical infrastructure. Are utilities, healthcare providers, airlines and food producers prepared to protect citizens from such a failure? What is the likelihood of such a scenario? What are the mitigation steps that should be taken—and with what level of urgency?





From a cyber-attack perspective, 2014 was a watershed year for a number of industries, including electric and power, healthcare, and financial services. For its part, the power generation industry has generally resisted the notion of vulnerabilities because of “air gap” controls between the Internet and power generation equipment, as well as the industry's heavy use of proprietary SCADA IP protocols.

This year, however, the power generation industry has finally had to acknowledge the increased threats and risks to normal service delivery. For example, it recently fell prey to a number of successful attacks, including the much-reported “Energetic Bear” malware report.

The power sector’s acknowledgement comes as other formerly “immune” industries are beginning to experience the perils of cyber-attacks. The financial service sector underwent an onslaught of exploitation to encryption protocol vulnerabilities, such as the BASH vulnerability. Boston Children’s Hospital became the first health care organization to be targeted by hackers.

The threats are real. The challenges are complex. But the klaxon is sounding—and we must take meaningful action to avoid catastrophes.

As more industries face complex threats, it’s a good time to revisit the acronym “C.H.E.W.”—which Richard Clarke, a former Special Advisor to the U.S. President on cyber-security, devised to categorize and explain the origin of cyber-attack risks:

-  **Cybercrime** – the notion that someone is going to attack you with the primary motive being financial gain from the endeavor.
-  **Hactivism** – attacks motivated by ideological differences. The primary focus of these attacks is not financial gain but rather persuading or dissuading certain actions or “voices.”
-  **Espionage** – straightforward motive of gaining information on another organization in pursuit of political, financial, capitalistic, market share or some other form of leverage.
-  **War (Cyber)** – the notion of a nation-state or transnational threat to an adversary’s centers of power via a cyber-attack. Attacks could focus on non-military critical infrastructure or financial services or more traditional targets, such as the military-industrial complex.

In the face of such daunting motives, it becomes clear how an average small company—a rural electric utility, for example—is vulnerable on multiple fronts. Such a utility may find itself inundated with attacks from customers protesting increases in service fees. It may be targeted by hackers who don’t condone its methods of power generation. Or it may fall prey to foreign intelligence operatives attempting to exploit a weak link in the nation’s power grid infrastructure.

The threats apply to players large and small—and the work ahead is both challenging and necessary. Stuxnet, Night Dragon, Shamoon, Dragonfly, Energetic Bear and other threats have already targeted critical infrastructures around the globe. They’re reminders of what we’ve experienced, as well as harbingers of what’s to come.

The threats are real. The challenges are complex. But the klaxon is sounding—and we must take meaningful action to avoid life-threatening catastrophes.

Our goal in this report is to provide actionable intelligence to ensure organizations can better detect and mitigate threats that plague their businesses. The report doubles as a resource guide that security professionals can easily reference and features recommendations that organizations can adopt to safeguard themselves against emerging attack trends and techniques.

## Most Important Findings

Radware's annual Global Application & Network Security Report outlines findings and analysis of the 2014 Security Industry Survey, incorporates our Emergency Response Team's (ERT) in-the-trenches experiences fighting cyber-attacks, and shares insights gleaned from our inaugural qualitative study of C-suite executives from multiple industries around the globe.

Designed to benefit the entire security community, this report provides a comprehensive and objective review of 2014 cyber-attacks from both a business and a technical perspective and gives best practice advice for organizations to consider when planning for cyber-attacks in 2015. It also offers a framework for understanding the "why" behind cyber-attacks—providing an orderly way to assess seemingly chaotic threats.

### What Changed in Security in 2014?

2014 was a watershed year for the security industry. Cyber-attacks reached a tipping point in terms of quantity, length, complexity and targets. Media coverage has kept pace, with plenty of coverage about the latest high-profile cyber-attack. But this report provides a big-picture view that is far more frightening than even the most ominous nightly newscast. Cyber threats are growing and expanding to new targets. The technical "bag of tricks" is bigger than ever, and hackers are combining "tricks" in new (and terrifying) ways. Even organizations with by-the-book security programs can be caught off guard.

### Attacks are Longer and More Continuous

In our 2014 Security Industry Survey, the **most commonly reported duration was one month** (cited by about 15% of respondents). However, **19% of the major attacks reported were considered "constant" by the targeted organization**. That's a stark contrast to the 2011, 2012 and 2013 surveys. While organizations reported many weeklong and even month-long attacks, never have more than 6% reported experiencing constant attacks.

This trend challenges the traditional concept of incident response, which assumes a normal state without attacks. It also exposes a security gap: When we asked respondents how long they could effectively fight an around-the-clock attack campaign, **52% could fight such a campaign for only a day or less**. Finally, while some experts are still emphasizing attack size, we consider that attribute akin to the color of a gun used to commit a crime. Given growing attack sophistication, size alone no longer has much bearing on effectiveness.

### No One Is Immune to Threats

As our Boston Children's Hospital case study suggests, threats have expanded to a broader range of industries, organizational sizes and technology deployments. In the [2014 Ring of Fire](#), four verticals—Education, Gaming, Healthcare and Hosting & ISP—advanced closer to the red-hot center. (See the ServerCentral case study for more on why security is becoming more complex and more critical for managed services providers.) Although Financial Services moved from "High" to "Medium" risk, most legacy industries remain at the same risk level.

### New Trends are Changing the Rules of the Game

In this year's report, we identify **three trends that we believe to be incredibly disruptive** to information security: the continued migration to cloud (and the accompanying dissolution of enterprise IT), the rise in the Internet of Things (IoT), and the move toward the software-defined network (SDN).

## Hybrid Solutions Gain Ground

This year, more than a third **(36%) of Security Industry Survey respondents indicated that they are already using a hybrid solution** with both customer premise equipment (CPE) and cloud solutions, while another 6% are planning to implement a hybrid solution. Interestingly, responses suggest that by 2015, **nearly half (48%) will employ hybrid protection.**

## Internet Pipe, Reflective Attacks Earn Dubious Honors

Radware's 2014 survey found that not only has it increased as a point of failure, **but the Internet Pipe now has the "honor" of being the number-one failure point.** Meanwhile, hackers seem to be making their way through every protocol to determine whether and how to use it for the next big reflective attack. The result: **Reflective attacks represent 2014's single largest DDoS "headache."**

## Headless Browsers, DDoS Attacks Become More Sophisticated

Attackers are now combining multiple techniques in a single attack—enabling them to bypass defense lines, exploit server-side vulnerabilities, and strain server-side resources. Such attacks include Anonymization and Masquerading, Fragmentation, Encryption, Dynamic Parameters, Evasion and Encoding, Parameter Pollution and Extensive Functionality Abuse.

## DDoS Remains Top—But Not Only—Concern

Continuing a four-year trend, **cyber-attacks were again split evenly between the network and application levels.** And while DDoS was the most-cited threat type (46%), its lead is narrow. Following closely are unauthorized access (41%) and advanced persistent threats (39%). Yet, with all of the threat types fairly well represented, the threat landscape appears to vary depending on each organization's industry and business concerns.

## Security Matters To C-Suite

In our qualitative study, nearly three-quarters of executives told us that security threats are now a CEO or board-level concern. In thinking about the top trends, cloud and BYOD were cited by more than one-third of executives who believe they increase security risks for their organizations. IoT was selected by more than a quarter of executives, while less than one-fifth cited SDN.

## Budgets Can Be Challenging—But Organizations Are Investing

Organizations of all sizes are struggling to finance and anticipate costs associated with cyber-attack prevention and mitigation. When asked how their organizations had deployed resources in response to cyber threats in the past 12 months, more than half of respondents reported changing security process, protocols and/or mandates, and nearly half said they had invested in new or specialized technologies.

This year's report illuminates how security attacks are becoming more complex even as macro-IT trends contribute to the dissolution of security effectiveness. Our research confirms that the motives, means and effectiveness of security attacks are on the rise—and highlights the need for greater agility to quickly adapt to evolving threats.



Through firsthand and statistical research coupled with front-line experience, this research identifies trends that can help educate the security community. The report draws its information from the following sources:

### **Security Industry Survey**

The quantitative data source is a Security Industry Survey, which was conducted by Radware and had 330 individual respondents. The survey was sent to a wide variety of organizations globally and designed to collect objective, vendor-neutral information about issues organizations faced while planning for and combating cyber-attacks.

39% of the companies in the sample are large organizations, each with annual revenue of more than US \$500m. A total of 23 industries are represented in the survey with the largest respondents from the following: telecommunications/Internet/cloud service provider (20.42%), financial services (13.15%), computer-related products or services (12.11%), and manufacturing/production/distribution (6.57%). About 40% of the organizations conduct business worldwide.

### **Security Executive Survey**

Alongside the industry survey, Radware selected eleven top security officers from an equal amount of organizations and conducted in-depth interviews about their experiences with cyber-attacks.

### **Emergency Response Team (ERT) Case Studies**

Radware's ERT is a group of dedicated security consultants that actively monitors and mitigates attacks in real-time, providing 24x7 security services for customers facing cyber-attacks or malware outbreaks. As literal "first responders" to cyber-attacks, Radware's ERT members gained their extensive experience by successfully dealing with some of the industry's most notable hacking episodes, providing the knowledge and expertise to mitigate the kind of attack that an in-house security team may never have handled. Throughout the report, the ERT team reveals how their in-the-trenches experiences fighting cyber-attacks provide deeper forensic analysis than surveys alone or academic research.





The Cyber-Attack Ring of Fire<sup>1</sup> maps vertical markets based on the likelihood that organizations in these sectors will experience attacks. The Ring of Fire reflects five risk levels—with organizations closer to the red center more likely to experience DoS/DDoS and other cyber-attacks and to experience them at a higher frequency.

Figure 1 illustrates that ten verticals fall within the Cyber-Attack Ring of Fire. Red arrows show which verticals have changed position since last year's report. This means that the overall number of cyber-attacks, as well as the frequency and intensity of these attacks has increased in 2014. Several verticals face consistent levels of threat, while just one—Financial Services—has actually moved from “High” to “Medium” risk. However, four verticals—Education, Gaming, Healthcare and Hosting & ISP—have advanced closer to the center of the Ring of Fire.

As companies move toward the center of the ring of fire, susceptibility to cyber-attack grows, creating a security gap.

As always, change brings risk. When a vertical shifts closer to the center of the Cyber-Attack Ring of Fire, companies in that industry are more likely to be the target of an attack. If mitigation assumptions still align with a previous position in the circle—in other words, a different level of risk—the likelihood of a cyber-attack resulting in a datacenter outage increases drastically. Organizations in verticals marked with a red arrow are wise to quickly adjust mitigation solutions to reflect the new risk level.

<sup>1</sup> The name has been changed from 2013's DoS/DDoS Ring of Fire to better reflect the current threat landscape.

## ⚠️⚠️⚠️ High Likelihood for Attacks

### Gaming

A longstanding target of cyber-attacks, gaming sites are very sensitive both to speed degradation and outage. They are also vulnerable when certain players become enraged over a financial loss. As unsuccessful players seek revenge, they are likely to pound the site with whatever is at their disposal—which, in many cases, is a DDoS attack.

In 2014, the experience of Radware's ERT shows that attacks were longer as well as "meaner." In all likelihood, these incidents did not result from a lone angry user. The more likely sources of these sustained attacks are competitive saboteurs, extortion-driven attackers or other entities with large capacities.

### Government

As the veritable "kings" of high risk, governments have always faced, and will always face, a high probability of cyber-attacks and DDoS threats. Events

in 2014—including the Ukraine-Russia conflict, Hong Kong protests, the shooting in Ferguson, Missouri, and the Israeli-Palestinian conflict—put relevant governments and federal agencies in immediate danger.

Fortunately, given their long history as high-risk entities, governments are relatively well protected. Their primary challenges today are keeping pace with attackers—as well as preparing for "APT-grade" attacks waged, or supported, by other governments.

### ISP & Hosting

For companies in the ISP & Hosting industries, 2014 was the year of the reflected attack. In addition to the older DNS vector, attacks targeted new ones—including NTP, chargen and SSDP (UPnP). This trend also dramatically increased both the volume of attacks and the number of attacks in the range of 10G to 50G. In 2014, such attacks became a common practice as they are easy to generate using the amplification technique. ISPs have been hit particularly hard by this trend. Although ISPs have long dealt with ongoing, low-level attacks targeting their customers, for the most part they have not had to worry much about such incidents. Now, however, the stakes are much higher. Targeting the ISPs—not their customers—attacks have become larger and potentially more effective.

Risk is on the rise for some unexpected targets: health and education. Likelihood of attacks is also heating up for gaming, hosting and isp companies.

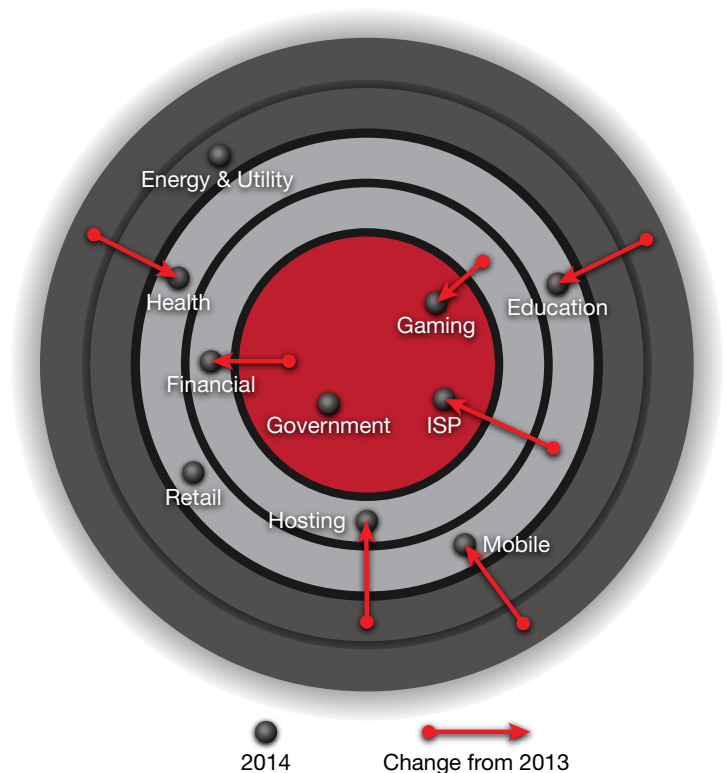


Figure 1: Cyber-Attack Ring of Fire

## ⚠️⚠️ Medium Likelihood for Attacks

### Education

Risk is heating up for educational organizations, as cyber-attacks become the modern-day equivalent of "The dog ate my homework." Students are launching attacks to buy more time for an assignment or, in a hacktivist-style move, to target the district or university following a disagreement with a specific instructor or administrator. The fact

that many educational systems rely on massive, interconnected networks—with dozens of schools tied to a single platform—only compounds the risk.

What's more, in the U.S. K-12 districts are finding that cyber-attacks can threaten their revenue streams. That's because federal dollars hinge on timely electronic submission of critical test results and other information. In 2014, a number of school districts experienced funding delays because cyber-attacks precluded submission of their data.

### **Financial Services**

After a few action-packed years—with attacks against stock exchanges in 2011 and against U.S. banks in OpAbabil in 2012 and 2013—2014 has proven to be a relatively “quiet” year. Prior-year experiences prompted banks and other financial institutions to enhance protection, leaving them in a fairly solid position.

But make no mistake: Financial organizations are still at a risk of attacks from various angles. Even when they are not government owned, banks serve as national symbols. In some countries they also symbolize capitalism in addition to providing the monetary component of any country's critical infrastructure. All of those factors can attract significant attention—and cyber-attacks.

### **Health**

The hacktivist attack on Boston Children Hospital (BCH) has provided clear evidence that even a wholesome and seemingly uncontroversial institution can find itself the target of an intensive cyber-attack. Through that 2014 attack, Radware's ERT witnessed firsthand what a cyber-attack can do to a hospital. And we realized what so many others have: When a hospital is attacked, lives are in jeopardy. Not surprisingly, the BCH case spurred discussion not only among security practitioners, but also within the medical community.

We believe the BCH incident cannot and should not be dismissed. It provides a clear message that every hospital is now at risk.

### **Retail**

Retail is holding steady, with a medium likelihood of attack. For retailers, threats typically arise from competitors, angry users, ransom plots professional hackers looking for financial gain and hacktivists who associate retailers with specific causes.

### **Mobile**

Before the rise of the smart phone, mobile devices were not subject to high-risk cyber threats. Even now, mobile users are not typically vulnerable to DDoS attacks. However, today's “mobile” devices include not only smart phones but also cellular modems attached to laptops, along with other remote or on-the-move equipment. For this reason alone, the threat has increased from Low to Medium. Meanwhile, keep in mind that DDoS can be a means to an end. Such attacks can affect mobile devices and users by shutting down security services that may protect the mobile unit from other types of attack vectors.

## **⚠️ Low Likelihood for Attacks**

### **Energy & Utilities**

For energy and utility companies, the threat landscape remains fundamentally unchanged from 2013 to 2014. These companies keep their core network functionality in isolated network segments—which has typically translated into safety from DDoS attacks. However, past attacks on these companies' public sites, intrusion attempts and other known incidents have proven that DDoS attacks on these networks are indeed possible. Thus, attack likelihood has increased and the potential impact of a successful DDoS attack introduces an overall high risk. One of the factors for this raise is the increased threat of cyber warfare.

# 04 | Business Concerns of Cyber-Attacks



When it comes to cyber-attacks, what consequences do organizations fear most? How are organizations quantifying the potential financial impact of a cyber-attack—and what kinds of solutions are they using to mitigate such incidents? Building on three years of prior research, Radware has once again surveyed security leaders to understand business concerns related to cyber-attacks.

## The Great Unknown - Attack Motivation

Overwhelmingly topping the list of reasons at nearly 70% - the motivation behind cyber-attacks remains shrouded for most organizations. Political/hacktivism still holds the second spot in the survey for the 4th year in a row cited at 34% with competition retaining the number three position cited at 27%. The list is rounded out by angry users and ransom attempts.

Which of the following motives are behind any cyber-attacks your organization experienced?

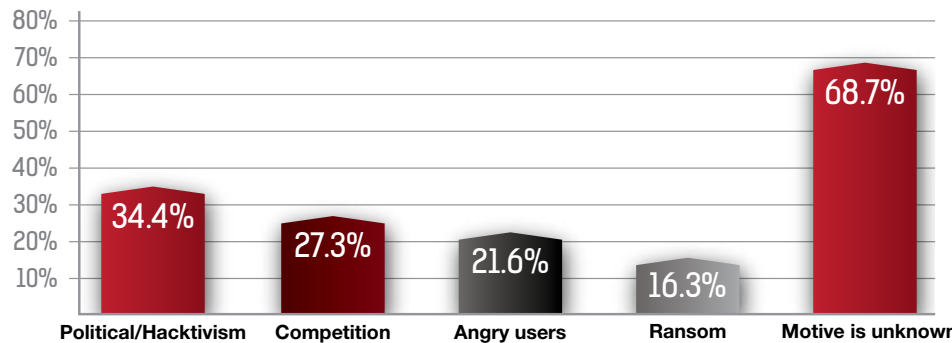


Figure 2: Motives behind cyber-attacks

What is perhaps most alarming about these stats is that 'unknown' still outpaces reasons in the 'known' category of cyber-attacks. Organizations are essentially left in the dark when it comes to the cause of the perpetration against them. In turn, this makes it harder for them to prepare for future attacks and makes the prosecution of attacks equally elusive.

## The Most Threatening Threats

In this year's Security Industry Survey, we asked which type of cyber-attack would cause the greatest harm to respondents' organizations. Nearly half of respondents pointed to DDoS attacks. Although DDoS was the most-cited threat type (46%), its lead is narrow.

Following closely are unauthorized access (41%) and advanced persistent threats (39%). Yet, all of the threat types are fairly well represented—suggesting that the threat landscape varies depending on each organization's industry and business concerns.

In your opinion, which of the following cyber-attacks will cause your organization the most harm?

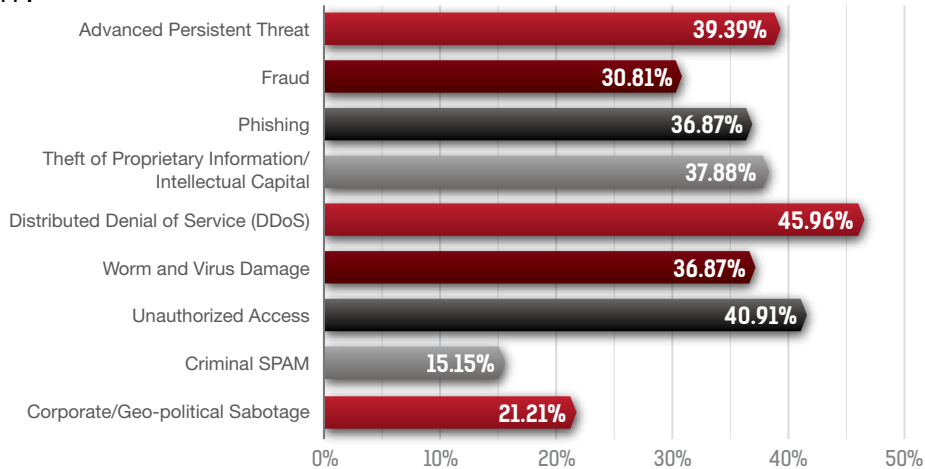


Figure 3: Attacks that will cause most harm to businesses

## Finding the Breaking Point

We also asked respondents about the average length of cyber-attacks experienced in the past year. The most commonly reported average duration—cited by just over 41% of respondents—was one hour. But nearly 14% told us their average is three hours, and nearly 10% said their attacks had averaged a month.

What is the average security threat your organization experienced?

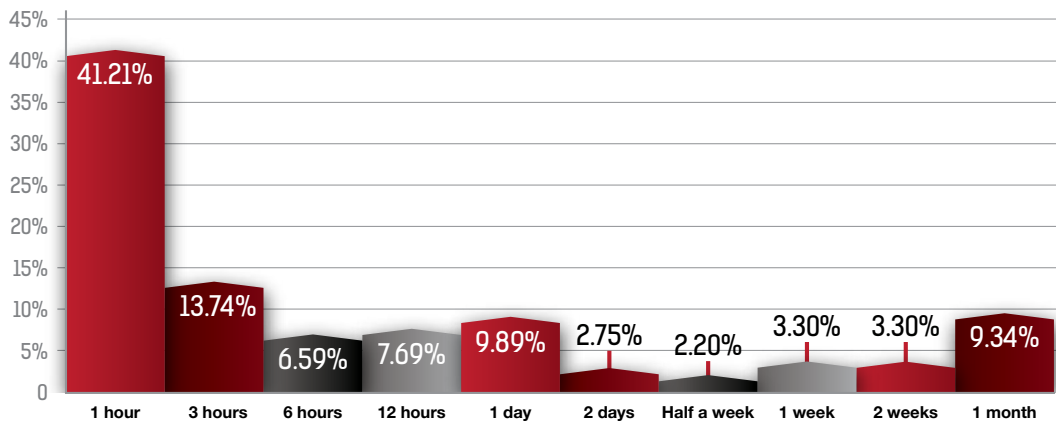


Figure 4: Average security threats

We also asked respondents about the maximum security threat their organizations experienced in 2014. The most commonly reported duration—cited by just about 15% of respondents—was one month. Conversely, nearly 14% told us their maximum threat experienced was just one hour, and over 13% said their maximum threat duration was three hours.

What is the maximum security threat your organization experienced?

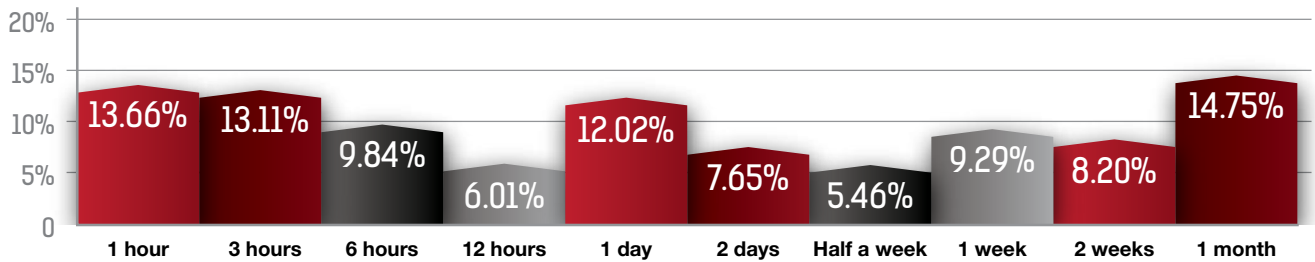


Figure 5: Maximum security threats

We also asked respondents how long they could effectively fight a round-the-clock attack campaign. The majority (about 52%) noted that they could only fight such a campaign for a day or less. However, about 35% believe they are prepared to withstand a round-the-clock attack campaign that lasts a week or longer, with 17% reporting being able to fight a month-long campaign.

How long can you effectively fight a round-the-clock attack campaign?

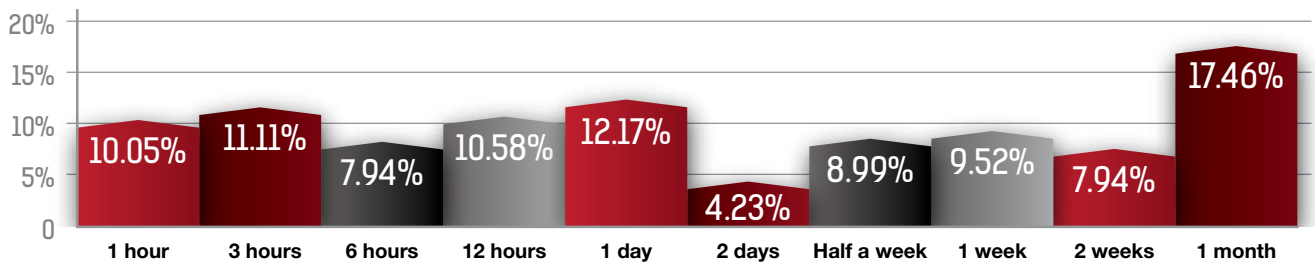


Figure 6: Effectively fighting round-the-clock attack campaign

## Most Pressing Concerns

In our 2013 Security Industry survey, respondents cited reputation loss and impact to internal organization/productivity loss as their top business concerns vis-à-vis cyber-attacks. In this year's survey, the top concerns are reputation loss and revenue loss.

What is the biggest business concern if your organization is faced with a cyber-attack?

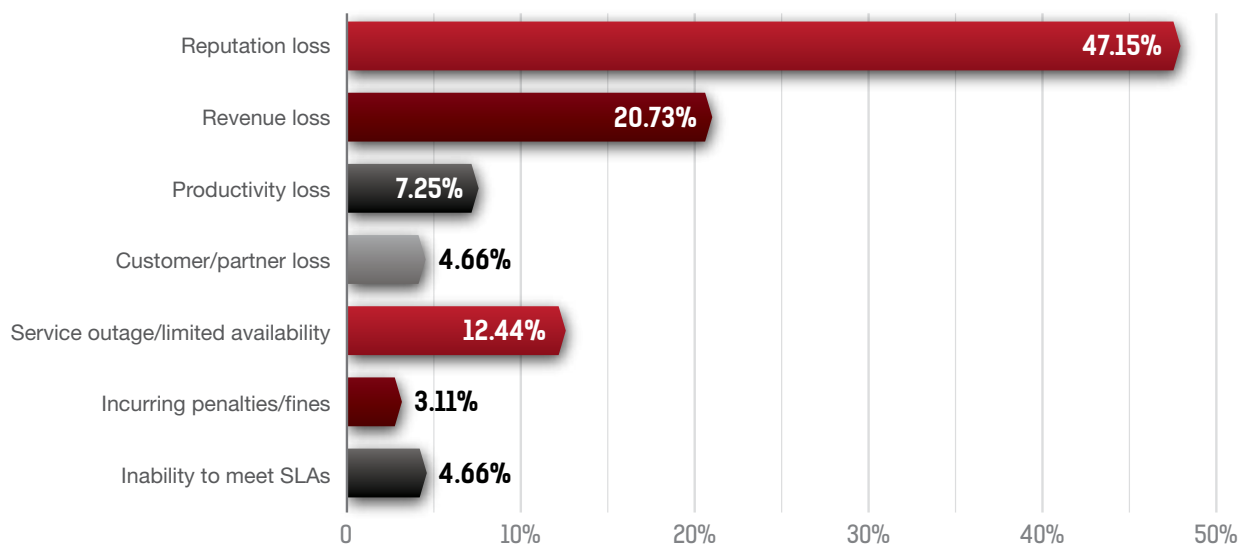


Figure 7: Business concerns due to cyber-attacks

## Budgeting and Planning

We asked the Security Industry Survey respondents about how their organizations had deployed resources in response to cyber threats in the past 12 months. More than half reported changing security processes, protocols and/or mandates, and nearly half said they had invested in new or specialized technologies.

During the last 12 months how has your organization responded to cyber threats?

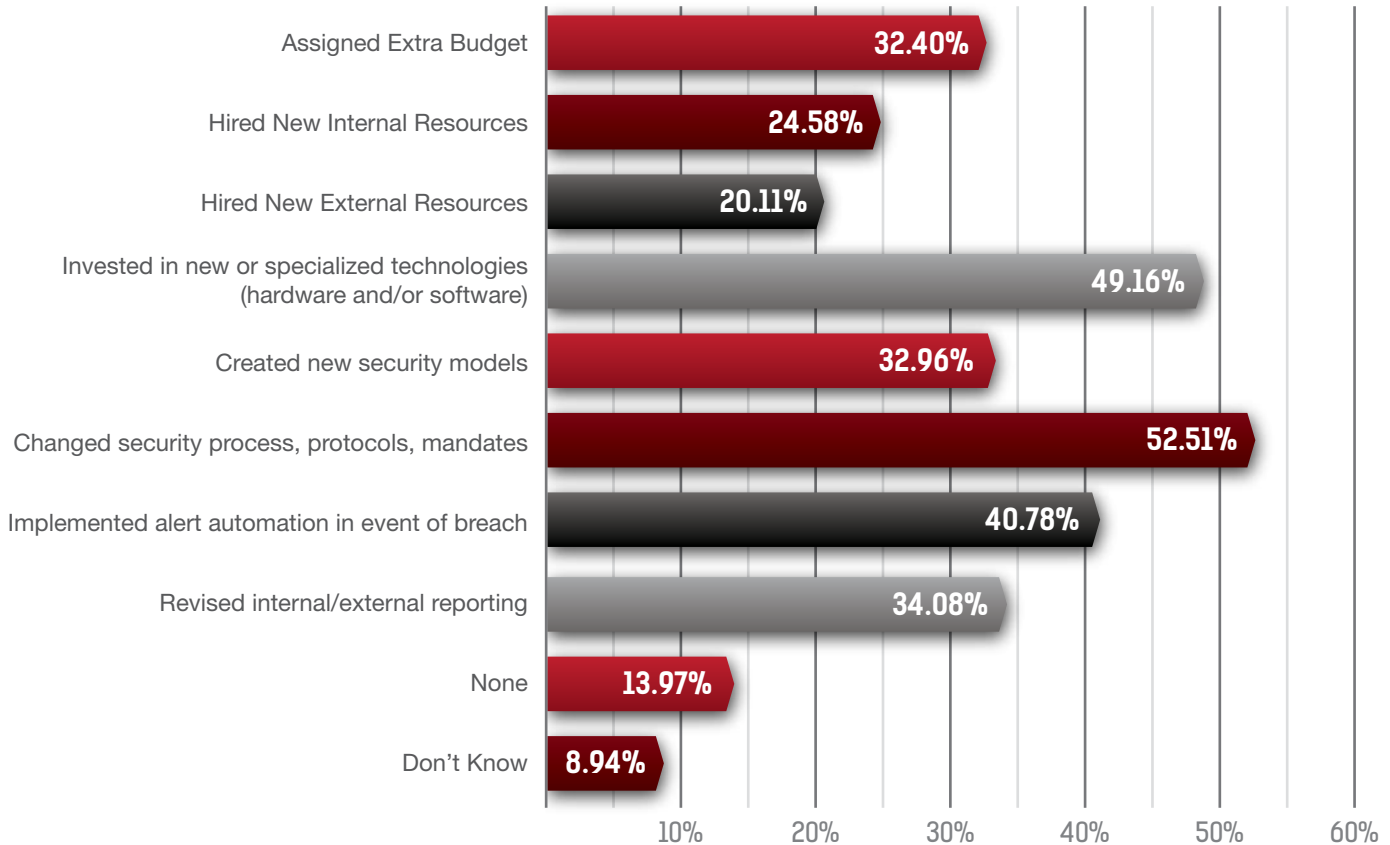


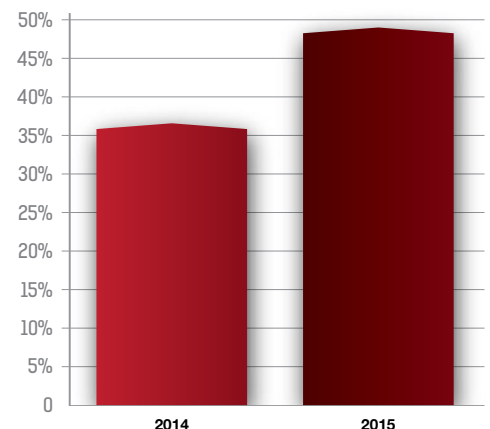
Figure 8: Responding to cyber threats

## Hybrid Protection for Cyber-Attacks

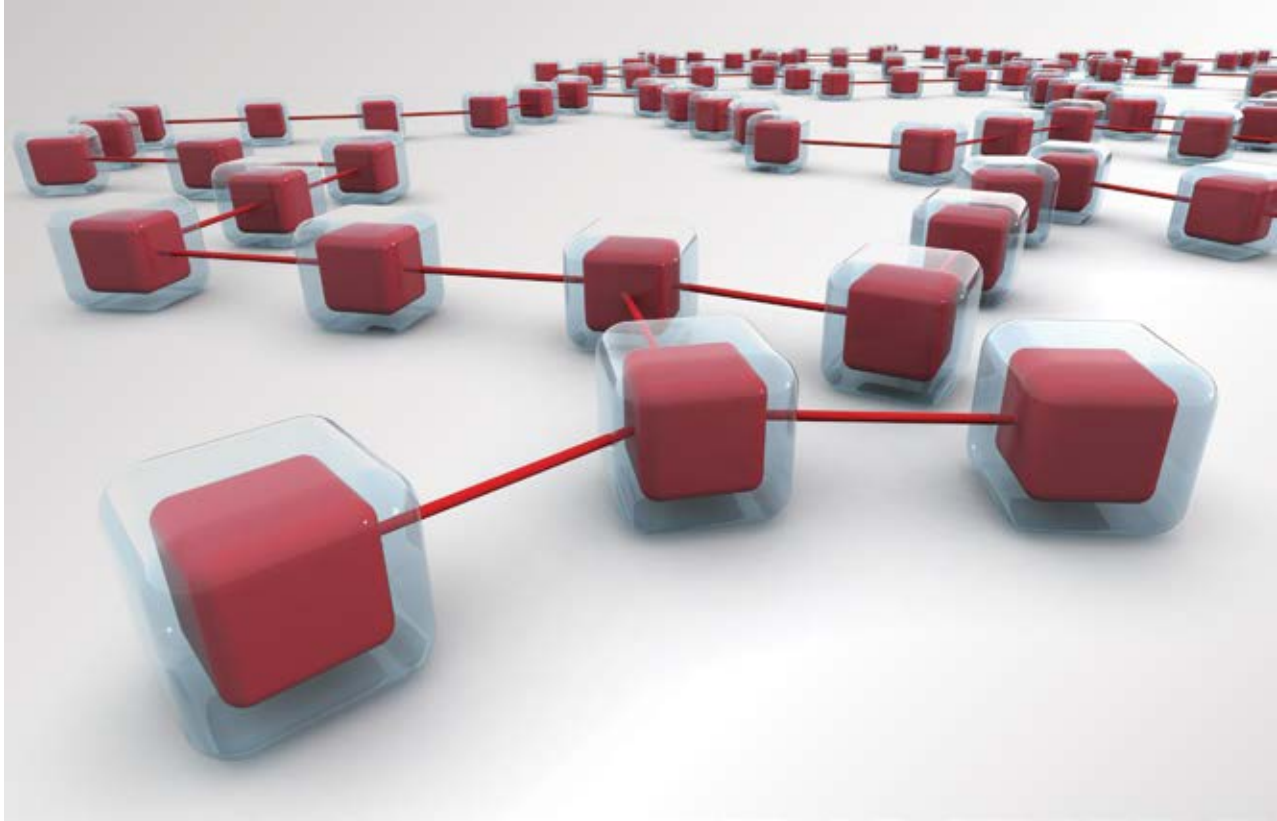
This year, more than a third (36%) indicated that they are already using a hybrid solution with both customer premise equipment (CPE) and cloud solutions, and another 6% are planning to implement a hybrid solution. Interestingly, responses suggest that by 2015, nearly half (48%) will employ hybrid protection. This trend aligns with Radware's longstanding position that a hybrid approach is optimal—a point of view that continues to gain momentum both in the market and within the analyst community.

We think the reasons are clear. With no other way to protect the cloud, cloud mitigation is a must. Meanwhile, on premise mitigation is essential because lower-rate attacks fly below the radar of cloud protection. The most notable example is SSL-based traffic, which can be meaningfully handled only after it is decrypted—a process that occurs inside an organization. Organizations remain unlikely to export their certificate to a cloud provider.

Figure 9: Organizations currently using and planning to use a hybrid security solution



# 05 | Attack Vector Landscape



Combining the experience of the Radware ERT and responses to this year's Security Industry Survey, this chapter reviews the various attack vectors that proved popular in 2014.

## Application vs. Network Attacks

In our annual security reports, Radware has maintained that network and application DDoS attacks have been—and will continue to be—balanced. That's because attackers' "interest" lies in multi-sector blended attacks. For example, a decent or even modest attack can include HTTP flood, UDP flood, SYN flood and/or a slow rate of attack. Thus, while there are each new attack "trends," there remains a stronger drive that balances this picture.

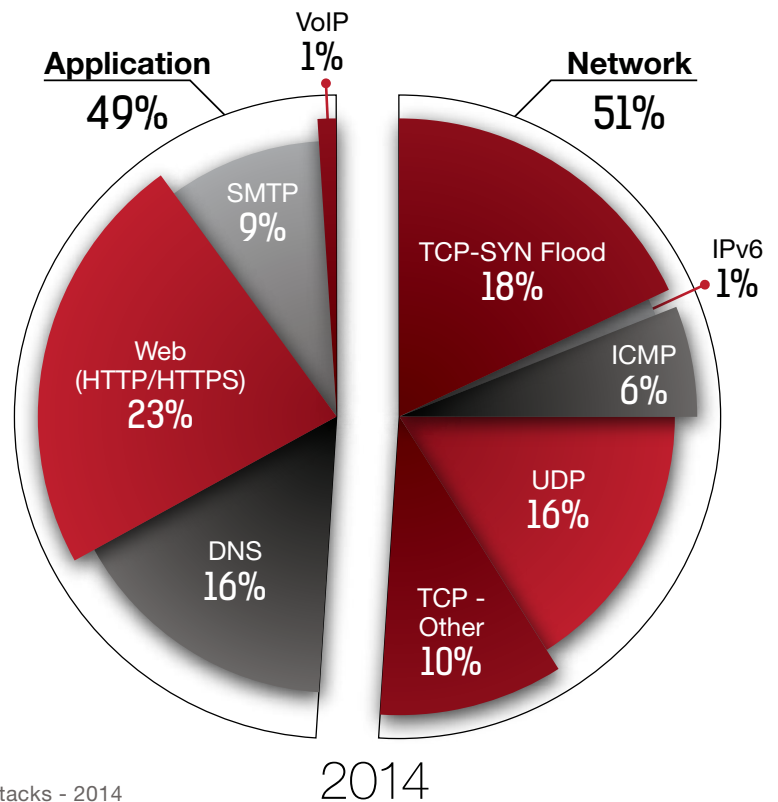


Figure 10: Network versus Application Attacks - 2014



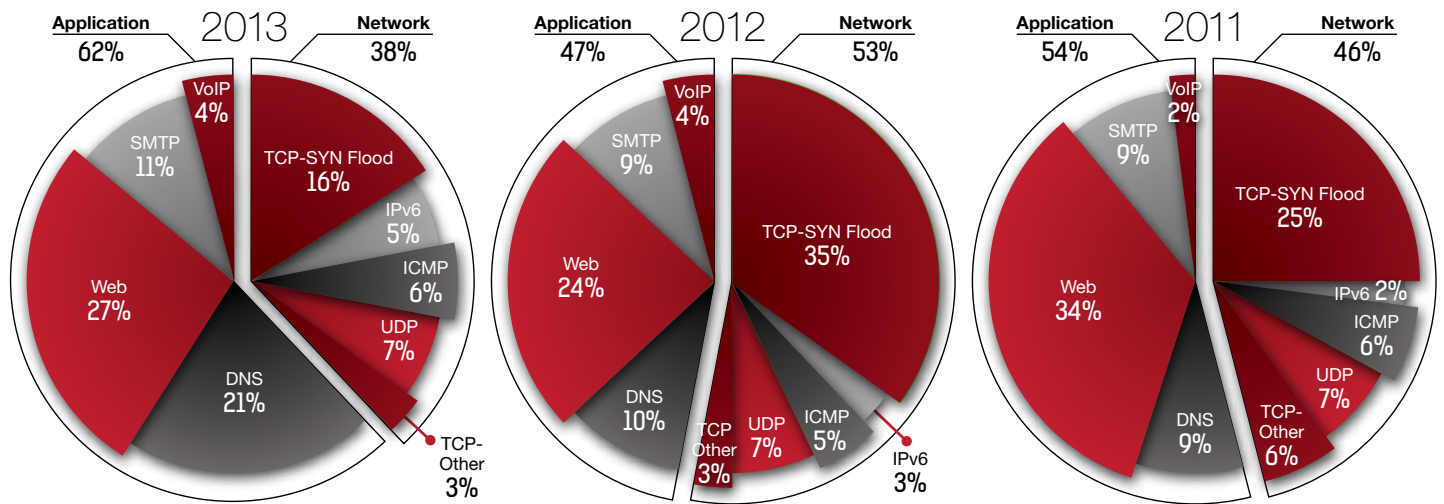


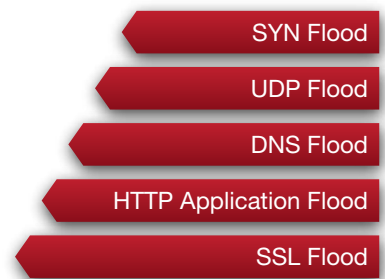
Figure 11: YoY diversity of cyber-attack vectors

It is perhaps unsurprising, then, that the 2014 results were evenly divided—with 51% of reported attacks targeting the network and 49% targeting applications. Compared to 2013, DNS attacks have decreased from 21% to 16%. While most of 2013’s reflected amplification attacks targeted DNS, NTP and Chargen joined the scene in 2014. Consequently, UDP attacks in general increased from 7% in 2013 to 16% in 2014. Meanwhile, web attacks remain the single most common attack vector; for every four web-based attacks, three target HTTP and one is an HTTPS attack.

Web attacks remain the single most common attack vector; for every four web-based attacks, three target HTTP and one is an HTTPS attack.

### Multi-Vector Attacks Become ‘Standard’ in 2014

In 2014, almost every attack campaign was composed of multiple attack vectors—so many that it can be difficult to track down all of the vectors. In many ways, it is no longer interesting to assess how much the quantity of per-campaign attack vectors increased in 2014. Multi-attack vector campaigns have become so commonplace that to have a campaign with a single attack vector is far more exotic.



Even so, ERT experience in mitigating attacks shows that vectors were different this year than last—simply because attack campaigns are now longer. In the past, most attack vectors were seen at the first day of the attack; today the defender must conduct different mitigation labor each day. That’s because nearly every time you successfully mitigate one attack vector, you know that tomorrow will bring a new challenge.

Although a layperson may consider DDoS an attack vector by itself, those well versed in the field of DDoS knows there are dozens, even hundreds, of attack vector variants and that attacks actually invent new variants. As an example, consider the Tsunami SYN Flood that ERT discovered in 2014. This attack vector is based on the classic SYN Flood; however, in this variant, the packets are not the classic data-less TCP SYN

packets. Instead, the attacks pad each SYN packet with about 1,000 bytes of data. Interestingly, the RFC does not even reject such usage. For the attackers, this vector is compelling because it allows them to carry a volumetric flood over the TCP protocol.

Another example of a “new” vector is manifested in the timely manner in which the attack initiates it. In 2014, the Radware ERT saw numerous campaigns in which the attack was generating a high-rate SYN flood for one minute and stopped for 15 minutes before resuming the pattern. In other cases, organizations would experience a very large volumetric UDP flood for three minutes, enjoy one hour of quiet and then experience another burst. To be sure, “bursty” attacks occurred prior to 2014. But thanks to heavy usage and the ability to synchronize the attack—reaching very high volumes in a short timeframe—these attacks became very prominent in 2014. With many organizations now protected against DDoS, attackers have found that bursty attacks can be more effective than constant ones. It sometimes takes several minutes for security measures to take full effect, and attackers have learned to use this to their advantage.

### Attack Strength and Duration Increase

To measure an attack, Radware uses a consistent formula based on three axes: attack duration, number of attack vectors and sophistication of the attack vectors. This formula yields the “DDoS Score,” which has helped illustrate how attacks are evolving to become longer, larger and more sophisticated. This is not an altogether new trend for 2014. In fact, results from 2013 and even 2012 underscored the growth in highly complex attacks with multiple attack vectors and rather long durations. What changed in 2014: Attack duration has increased and extra-large attacks have become common.

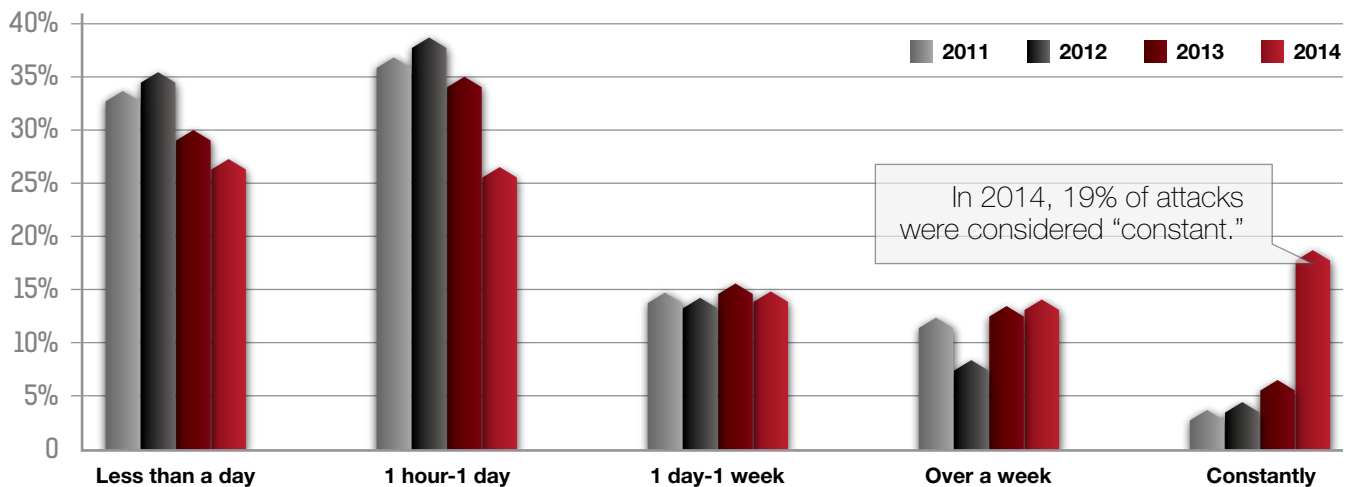


Figure 12: YoY attack durations

In 2014, a number of Radware ERT customers experienced very long attacks. Survey results echo that experience, with 19% of the major attacks reported considered “constant” by the targeted organization. In past years (2013, 2012 and 2011), organizations have reported many week-long and even month-long attacks—but never have more than 6% reported experiencing constant attacks.

Radware considers any attack in the range of 10Gbps to 100Gbps to be “extra large.” While some may infer based on high-profile cases that such attacks have long been commonplace, in reality they have been quite rare even as recently as 2013 and 2012. After all, since many organizations are unable to withstand even a 1Gbps attack, why generate more?

However, 2014 experience and survey data suggest that the landscape is changing. The Radware ERT reports seeing extra-large attacks on a daily basis—and that these attacks are targeting all types of organizations. We believe the longer, higher-volume attacks are not due to an increase in sophistication (or a suddenly stronger desire to pinpoint the “crack in the wall”). Rather, we believe this trend is arising from the “better” technology—namely, reflected attacks—at attackers’ disposal. Reflected attacks make it comparatively easy not only to generate an extra-large attack but also to sustain it for an extended period.

### Attack Size: Does It Matter?

Many security officers focus on preparing for attacks in the gargantuan, 100Gbps size range. But an over focus on these attacks can be potentially short-sighted or dangerous. That’s because it misses the complexity of the DDoS threat. In reality, security officers would be wise to prepare for a more complex landscape of threats: volumetric attacks larger than their pipe size; application attacks, which may not stand out in terms of bandwidth but can target specific critical resources; and “low and slow” attacks that may occur below the radar, making them difficult to detect based on bandwidth alone.

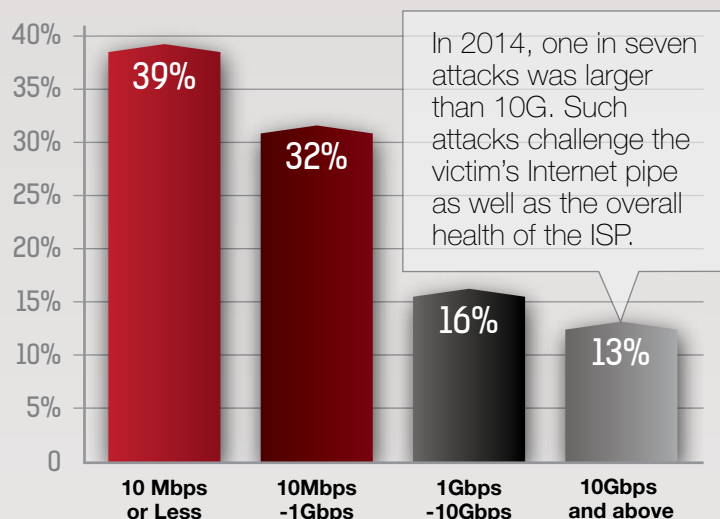


Figure 13: Bandwidth of Server Attacks

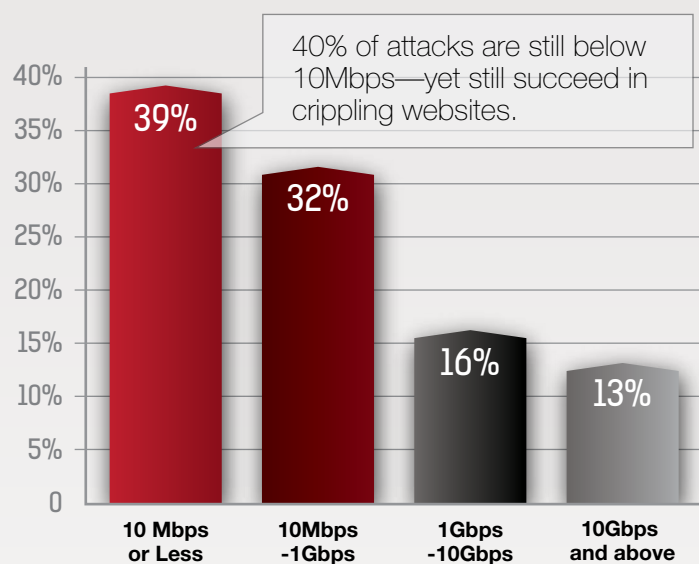


Figure 14: Bandwidth of Server Attacks



## 06

### Headless Browsers and DDoS - Attacks Become More Sophisticated

Web applications accessible via the HTTP protocol face numerous challenges when it comes to mitigating denial of service (DoS) and distributed denial of service (DDoS) attacks. As organizations have adapted by employing dedicated anti-DDoS solutions, attackers have followed suit. In this chapter, we review key milestones in the evolution of attacks in the HTTP layer and discuss the increasingly sophisticated threat from headless browsers.

Denial of service attacks may target various players in a web application's multi-tiered architecture. Targets may include the way that the web server handles the HTTP protocol itself or the web server's CPU, storage resources, or interaction with a database or other entities. The goal of DoS attacks is to exhaust a web application's limited resources, thereby damaging users' experience or by taking the website down.



Figure 15: LOIC Denial of Service Tool

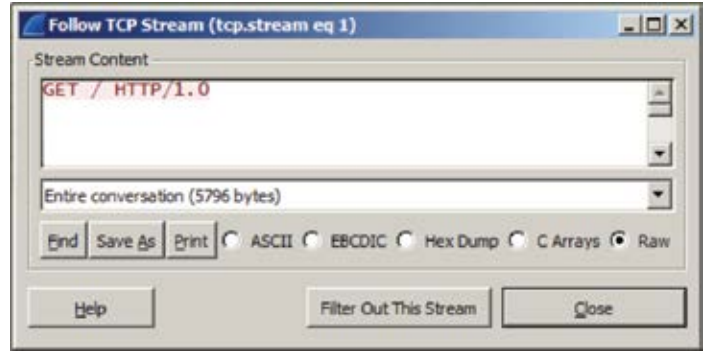


Figure 16: HTTP GET Request Generated by LOIC

For example, the HTTP GET flood is a common attack. In this attack, the attacker generates multiple HTTP GET requests in order to strain the web servers' and databases' connection pools, the bandwidth, and even the CPU. Low Orbit Ion Cannon (LOIC) is a denial of service tool that rapidly generates simple HTTP GET requests.

A closer look at the GET request shows that it sends a minimal GET method with no HTTP headers.

## A Cycle of Mitigation and Adaptation

Anti-DDoS solutions quickly responded by inspecting incoming traffic and checking that HTTP requests contain HTTP headers (a valid user agent and host header, for example). If headers were missing or illegal, the anti-DDoS solution would deem this traffic malicious and not pass it to the web application.

Attackers analyzed the mitigation and adapted by adding valid headers to their HTTP GET requests. Moreover, to avoid static signature detection, some tools—including the High Orbit Ion Cannon (HOIC)—include an option to send different header combinations based on a user-supplied list of valid headers.

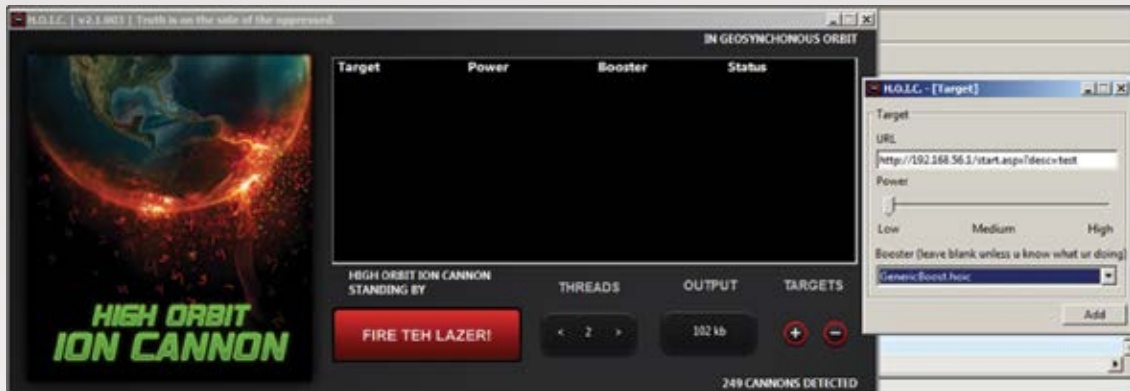


Figure 17: HOIC Denial of Service Tool

Notice the differences generated by the tool in the Referer and User-Agent headers.

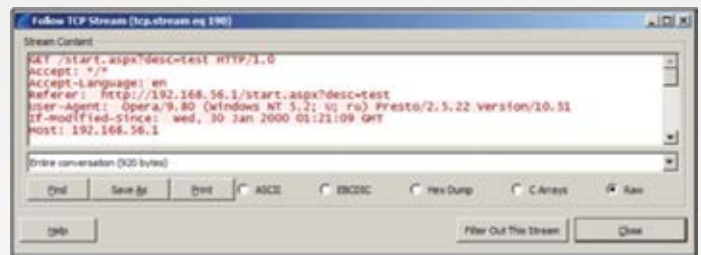
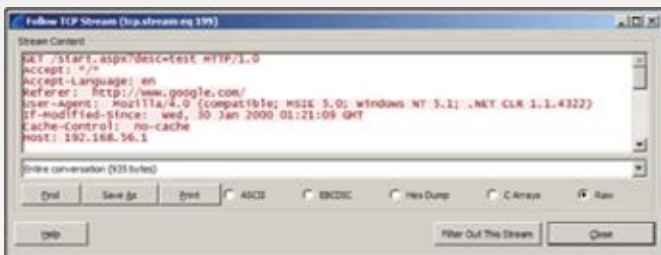


Figure 18: HOIC Changes in the Referer and User-Agent Headers

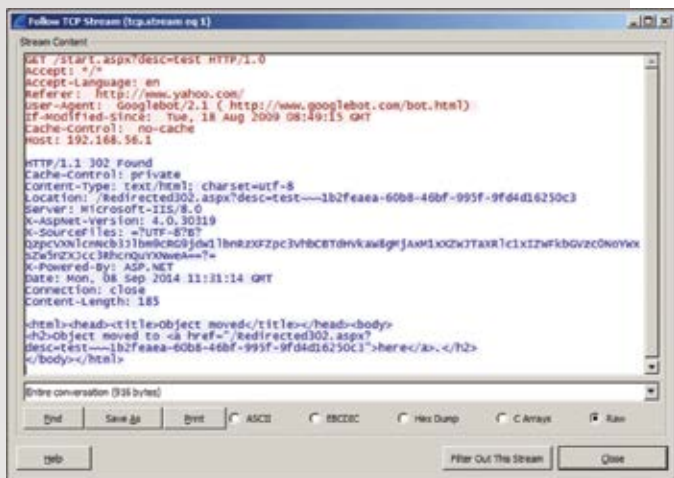


Figure 19: HOIC-Generated HTTP Fails the 302 Redirect Challenge

At this stage, anti-DDoS solutions employed another quick safeguard before passing the traffic to the server. They would present a CAPTCHA challenge to the incoming request. However, this approach negatively affected users' experience and therefore was quickly limited to extreme cases.

Anti-DDoS solutions then had to take a new approach—differentiating between real users and automated traffic by relying on the behavior of the tool that real users employ: the web browser. Browser behavior provided a new mechanism for detecting suspicious traffic by issuing HTTP challenges.

### Initial HTTP Challenges

The first HTTP challenge to be addressed is the 302 HTTP response code. This code instructs the client to follow a redirect presented in the HTTP response in order to reach the desired resource on the web application. Simple scripts and dedicated DDoS tools are programs that are designed for specific tasks. Thus, they do not follow the redirection—and do not reach the web application. While it's possible to extend these scripts and tools to handle every HTTP response, as a browser would, it is not worthwhile from the attackers' point of view.

An HOIC-generated HTTP flood does not follow a 302 HTTP redirect.

### Second-Generation HTTP Challenges

Another key challenge was client-side HTTP cookie handling. Anti-DDoS solutions instruct the client to establish an HTTP cookie. They also check if subsequent requests contain a valid HTTP cookie.

Once more, attackers developed new techniques to adapt to the 302 HTTP and cookie challenges. To that end, they adopted available URL retriever tools that can handle these challenges (for example, curl and wget).



Figure 20: URL retriever tools to handle cookie challenges

### Third-Generation HTTP Challenges

By this time, defenders had to devise a new technique for differentiating between traffic originating from legitimate users and traffic originating from URL retrievers, such as the aforementioned curl and wget.

The new HTTP challenge set in the response was a dynamic JavaScript challenge. In this challenge, the client automatically parses JavaScript code and sends to the server a new request with indication markers that it was able to parse and executed the JavaScript code.

The ability to parse JavaScript code is not inherent in standard URL retrievers. Consequently, the connection stream ends in this challenge.

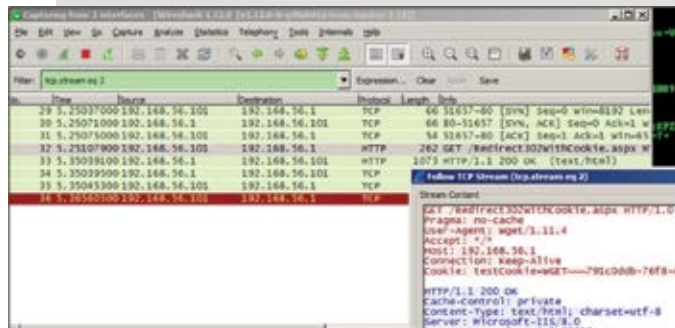


Figure 21: WGET Tool Fails the JavaScript Challenge

### Fourth-Generation HTTP Challenges: Headless Browsers Emerge

Eager to bypass to third-generation HTTP challenges, attackers sought ways to imitate browser behavior as much as possible. For that reason, DDoS attacks started to use “headless browsers.” Headless browsers, such as PhantomJS and HTMLUnit, are tools that function as a browser but without a graphical user interface (GUI). Test automation is the most common use of headless browsers thanks to their ability to automatically parse and execute dynamic content, including JavaScript, as a browser would.

To mitigate this sophisticated attack, Anti-DDoS solutions employed the mouse move challenge. At time of writing, DDoS tools could not support this functionality. With a simple script, PhantomJS easily bypasses all challenges but is stopped at the mouse move challenge.

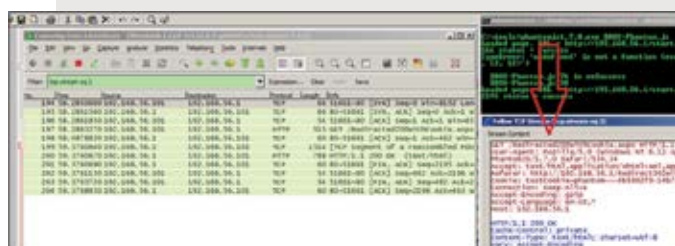


Figure 22: Headless Browser – PhantomJS Fails the Mouse Move Challenge

### Next-Generation HTTP Challenges

Headless browsers are evolving rapidly. With the help of the community, open-source extensions, such as CasperJS, are capable of passing all of the aforementioned HTTP challenges, including the mouse move challenge. Consequently, they can bypass the anti-DDoS solution’s radar and successfully masquerade as legitimate traffic.

This kind of sophisticated attack is not common. Thus, next-generation challenges will have to identify and synthesize such automatic infiltrators.

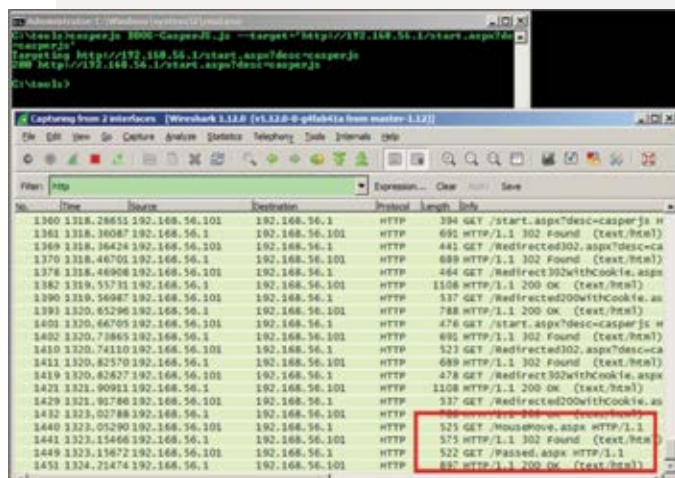


Figure 23: Headless Browser – CasperJS Bypasses the Mouse Move Challenge

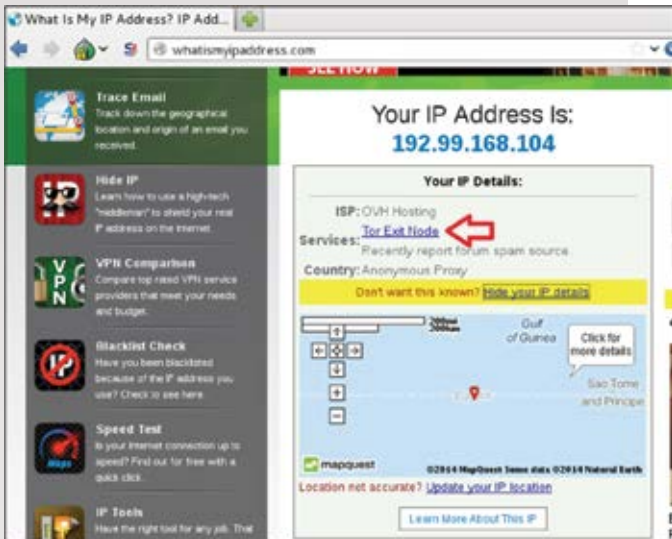


Figure 24: Tor Anonymization Proxy

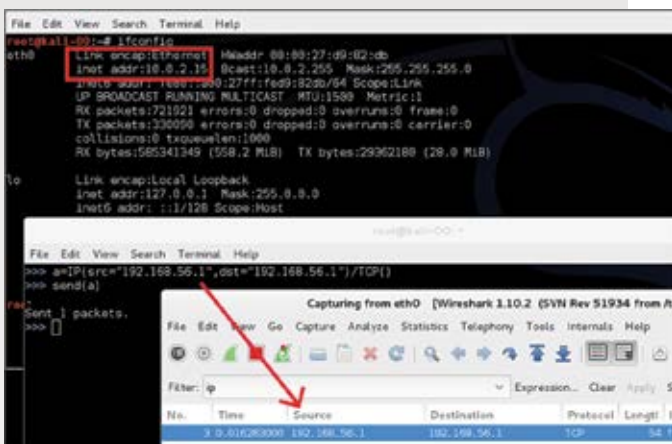


Figure 25: Masquerading in IP Source Port



Figure 26: Masquerading Values in HTTP Header User-Agent

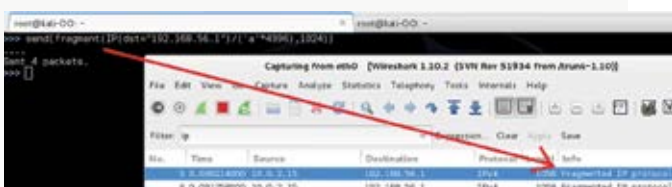


Figure 27: Fragmentation of Packet

## Mixed Attacks Are on the Rise

As organizations have adopted multiple mechanisms for cyber defense, attackers have adapted. By combining multiple techniques in a single attack, they're able to bypass defense lines, exploit server-side vulnerabilities, and strain server-side resources. This section reviews how they can be combined to thwart an organization's cyber defense.

## Anonymization and Masquerading

A simple solution to mitigate an attack is to block traffic from a malicious IP or unauthorized clients. Thus, attackers hide their IP addresses behind an Anonymization proxy and service, such as Tor.

While it's possible to discern traffic that originates from the Tor network, not every organization wishes to block this traffic.

Another technique for hiding IP addresses is changing fields in the communication, such as the IP source address, or values in the HTTP header user-agent.

In the first quarter of 2014, attackers abused the WordPress pingback functionality—instructing about 160,000 WordPress websites to send an HTTP GET request to a victim's website.

Another common approach that attackers use to conceal their origin: launching the attacks from remote compromised hosts, often via amassed botnets.

## Fragmentation

Packet inspection mechanisms look for patterns in a given packet. Attackers can bypass this detection by fragmenting the packet into several smaller packets. In addition to compounding detection challenges, fragmentation also strains the security systems that must defragment traffic in order to handle this evasion. High rates of fragmented traffic therefore put security infrastructure itself at risk.



## Encryption

A growing number of attacks are targeting resources accessible over the Secure Sockets Layer (SSL). As a result, traffic is encrypted and defense mechanisms are often unable to inspect it. In these cases, defense mechanisms proxy the Transmission Control Protocol (TCP) payload without performing a real inspection.

When defense mechanisms actually perform SSL decryption, they incur risk associated with heavy processing of the decryption and encryption. That processing places a significant burden on the SSL server-side computational and memory resources. Thus, many attackers add encryption to increase the strain rather than to actually evade detection.

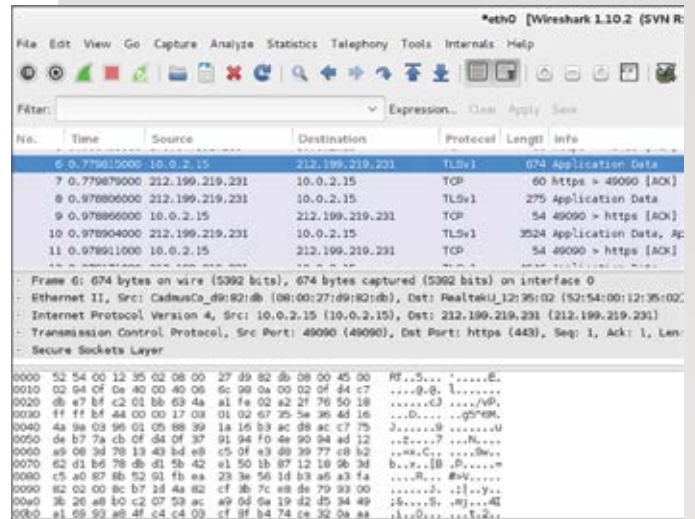


Figure 28: Attack Targeting Resources Accessible over the SSL

## Dynamic Parameters

Another attack technique is repeatedly transmitting the same attack along with different parameters. Dynamic parameters eliminate the effectiveness of complete packet static signatures and content delivery networks (CDN), as they would deem each transmission “new.” Because CDNs automatically forward dynamic content to the origin server, they can be completely bypassed in this way.



Figure 29: Dynamic Parameters Attack

## Evasion and Encoding

At their core, evasion techniques are about sidestepping problems. One example is encoding the payload.

Attackers avoid detection by encoding the payload in various ways: HTML encoding, URL encoding, or double encoding. For example, instead of sending `javascript:alert(/xss/)`, attackers URL encode the payload twice. The defense mechanism decodes the payload once, searches for a malicious pattern, and then forwards it to the backend server. The backend server receives the payload, decodes it again, and runs the malicious payload.

Detecting such mechanisms requires full normalization of the HTTP traffic—another resource-intensive operation that many security systems don't perform.



Figure 30: Evasion Technique - Encoding the Payload

## Parameter Pollution

In some instances, the algorithm within a defense mechanism inspects values in specific locations while the backend server reads the value from a different location. In this case, attackers can send an SQL Injection payload, which will be executed at the backend database.

## Extensive Functionality Abuse

The endpoint destination of an attack is a key contributor to the success of the attack. Attackers are looking for functionalities that, when executed, require heavy server-side resources. Once identified, attackers flood these resources with numerous requests, straining the server to or beyond its limits.

For example, an HTTP GET flood on different pages of the same web application will yield different results. The first flood is carried against a default static homepage. Meanwhile, the second targets a website's search feature. In the attack against the static homepage, the server can quickly send a response; that's because generating the static responses requires minimal resources. On the other hand, the same web application that receives requests to perform a search over SSL requires additional server-side resources to perform the search operation and handle encrypted transmissions.

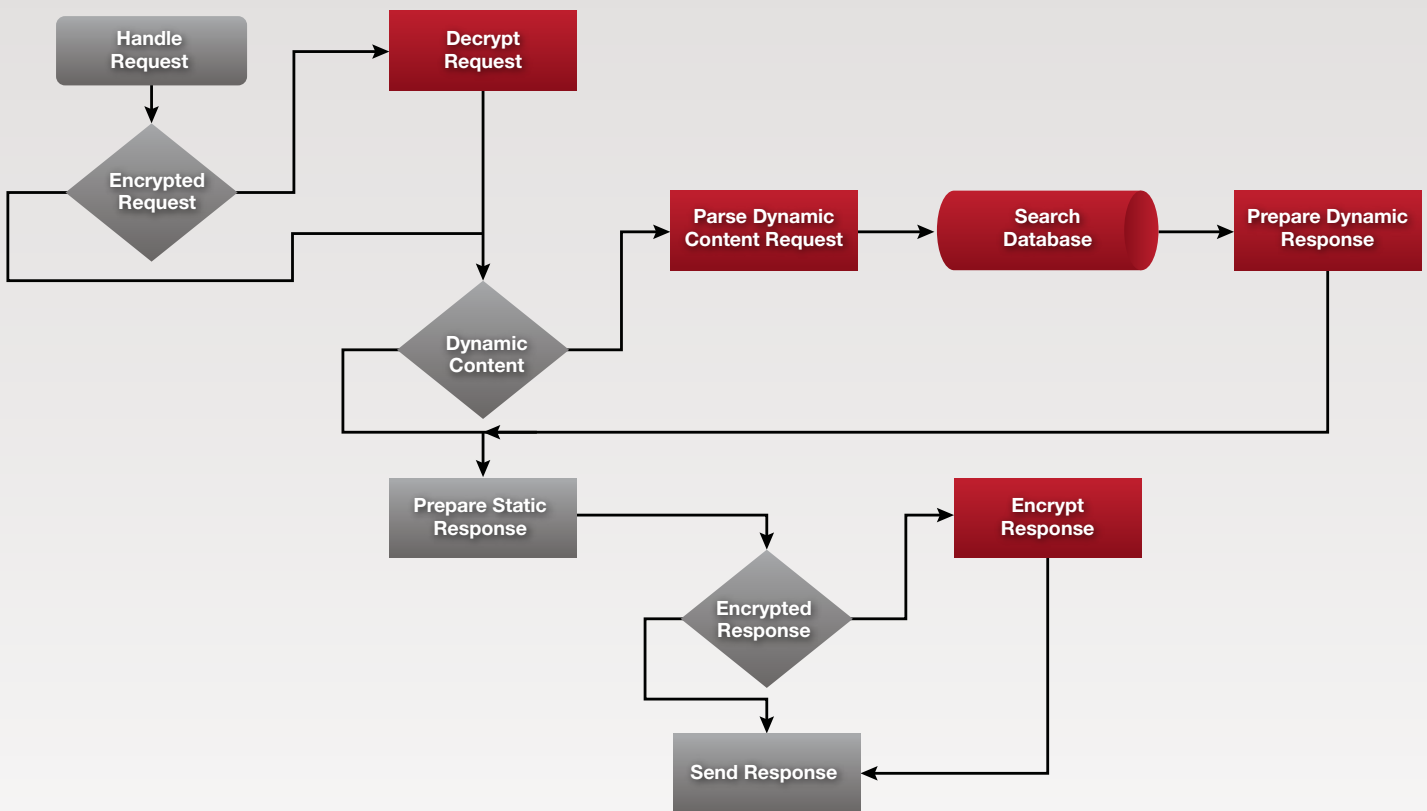


Figure 31: Additional Operations (in red) Required for Encrypted Dynamic Response Generation

## Demonstrating a Mixed Attack: The Whole is Greater Than the Sum of Its Parts

Reviewing several attack techniques reveals that while each is harmful when arriving separately, the damage is compounded when the same techniques are combined.

This simulation analyzes how a mixed-technique DDoS attack against the Damn Vulnerable Web Application passes organization's defense lines and strains the backend server's CPU resources to 99.9% per single request.

The first step is analyzing a capture of the suspected traffic.

From this capture, it is clear that the traffic is encrypted.

Thus, several defense devices could not analyze the traffic to detect malicious patterns. Decrypting and inspecting the traffic would require additional resources.

Analysis of decrypted traffic reveals the malicious request sent to the server.

The payload shows that the attack is SQL Injection on a web page that receives input from the client. Why was this attack not mitigated by the organization's web application firewall (WAF)?

The payload avoided mitigation by using the following techniques:

1. The attack targets a dynamic page, thus requiring additional server-side computing resources, such as CPU and database operations.
2. The green and red shows that the id parameter is duplicated. The payload in the red text indicates that the second id parameter contains the SQL Injection payload while the value in the green id contains a legitimate value.
3. Because the id parameter is configured to accept one value, spaces are not allowed. The attacker wants to insert a full SQL statement, so he or she used the `/**/` comment marker, which are equal to spaces. Thus, this comment marker allows the attacker to insert several directives into a full SQL statement while still being interpreted as one value in the id parameter.
4. The attacker uses the `||` combination instead of the SQL OR directive, which can be picked by pattern matching.
5. The `sha1(0x61)` instructs the server to calculate the sha1 hash of 0x61. 0x61 is text encoded in hexadecimal which is used as an evasion technique for sending text without using comma separators. It stands for the character "a".
6. The `/*!5000payload*/` is another pattern evasion technique designed to escape regular expressions searches for the BENCHMARK keyword.
7. The BENCHMARK function instructs the database to perform an action a certain number of times.

Putting it all together, the attack payload instructs the database to **calculate the sha1 hash of the "a" character 999, 999, 999 times per single incoming request**. The impact of this attack was denial of service for the server due to heavy, repetitive database operations.

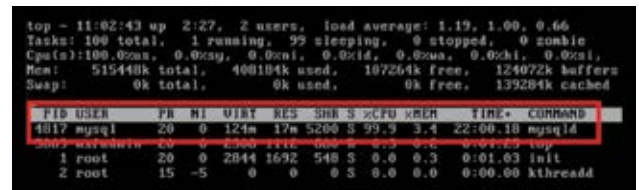


Figure 32: Mixed-Technique DDoS Attack against Damn Vulnerable Web Application

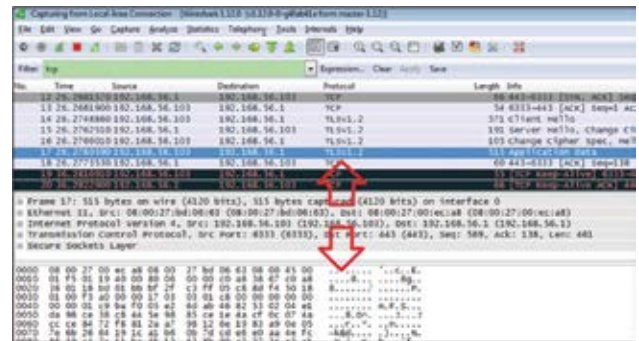


Figure 33: Analyzing Suspected Traffic



Figure 34: Analysis of Decrypted Traffic Reveals Malicious Request Sent to Server

## Points of Failure

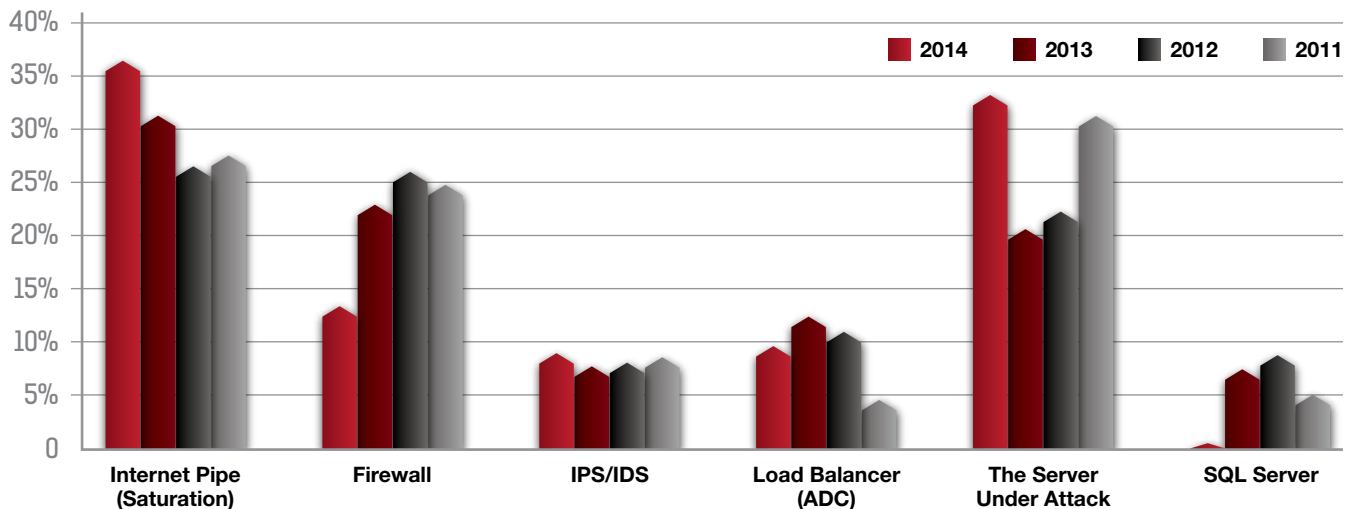


Figure 35: Which services or network elements are (or have been the bottleneck) of DoS?

In 2011, Radware started surveying security leaders about the point of failures in DDoS attacks. Every year, the results have been largely consistent: Points of failure are divided among three main entities. The most obvious, of course, is the server that is under direct attack. However, the Internet pipe itself becomes a point of failure when it gets saturated, and the firewall—a stateful device—often fails even sooner than the server.

In our 2014 survey, we found that the Internet pipe has increased as a point of failure. In fact, it has the dubious honor of being the number-one failure point—most likely because of the increase in User Datagram Protocol (UDP) reflected amplification attacks.

## Reflected Amplified Floods Remain a Key Challenge

Ten or twenty years ago, DoS attacks mostly targeted the network through SYN, TCP, UDP and ICMP floods. The years 2010-2012 brought an increase in a more sophisticated application attack, with some experts heralding the demise of network attacks. (For the record, Radware has always asserted that there would be a balance between the two.)

More recently, a specific type of DoS attack—the amplification reflective flood—has not only revived network attacks but also given them an edge over their counterparts that target applications.

Reflective attacks, including those using DNS, NTP, and CHARGEN, started heating up in 2013 and remained a persistent threat throughout 2014. Reflective amplified attacks appear deceptively simple. What makes them effective is the ease with which they can be generated—and the impact they can have on a network.

“NTP and DNS amplification attacks are the most common attacks seen on our network. We have experienced degraded services and acquired new protection as a result.”

*Dannie Combs  
CISM Senior Manager  
Network Security  
US Cellular*

Type	Amplification Factor	Amplification Methods
DNS Reflective Attack	x5-x100	By nature, Domain Name Service (DNS) has a x5 amplification factor. Using 'ANY' or another crafted amplification, means it can reach as high as x100.
NTP Reflective Attack	X300	Network Time Protocol (NTP) is an important protocol for time synchronization. Its MONLIST command can generate a response that is x300 the request.
CHARGEN Reflective Attack	x50	Commonly used with Transmission Control Protocol (TCP), the CHARGEN receives a one-byte stream for testing purposes. However, it also supports User Datagram Protocol (UDP) and generates x50 larger responses.
UPnP SSDP	x30	Universal Plug and Play (UPnP) and particularly the Simple Service Discover Protocol (SSDP), which allows network devices to get "acquainted."

Hackers seem to be making their way through every protocol to determine how to use it for the next big reflective attack.

To compound the pain, 2014 brought a rise in the popularity of volumetric attacks. Truly high-volume attacks—that is, those that are more than 10Gbps—were uncommon in previous years. That situation has changed in 2014, however, with many organizations facing the threat of attacks larger than 10Gbps. In fact, attacks that are 20Gbps to 50Gbps are not out of the ordinary—making volumetric attacks one of the key threats that organizations must understand and prepare for.

Interestingly, high-volume attacks affect large organizations more than small ones. For a small organization with a 100Mbps line, the size of the volumetric attacks is irrelevant. Whether the attack is 100Mbps, 1 Gbps or even 10 Gbps, the organization will need an external security service to protect it. The situation is quite different for large entities, which faced little threat from 100Mbps attacks. Once attacks exceeded 1G, they became an issue.

High-volume attacks are especially worrisome for carriers. For a carrier, a 50 Gbps attack on one of its end customers doesn't go unnoticed. With such high-volume attacks hitting more frequently—sometimes, even a weekly basis—carriers faced the need to protect not only the individual targets but their entire network.

“As a result of reflected amplification attacks (DNS, NTP, etc.) our organization had to acquire new protection.”

*VP Information Security  
Strategy & Development,  
U.S.-based, Fortune 1000  
financial services company*

# Three Incredibly Disruptive and Immutably Macro-Trends in Information Security



Today's business environment offers plenty of reminders that a macro business trend can arise seemingly out of nowhere and render companies—and, in some cases, whole industries—obsolete. Remember when Sony ruled portable music? How about “innovative” productivity tools like Smith-Corona typewriters or, more recently, Palm personal digital assistants and BlackBerry cell phones? In the face of disruptive technologies, those and many other products have gone the way of the horse and buggy because they didn't recognize a threatening macro-trend—or were simply unable to adapt in time.

As information security professionals, we are not immune to the effects of seismic shifts in technology. This section explores three incredibly disruptive and immutable macro-trends affecting information security. It also makes a strong recommendation: Don't become obsolete by ignoring or resisting these trends.

## That Was Then

Businesses across industries have deployed automated systems and processes in the name of speed, efficiency and competitive advantage. For the past 20 years, information security professionals and technologies have worked to thwart a landscape of threats targeting those investments. For the most part, both these automated systems and the security tools designed to protect them reflected longstanding assumptions about how businesses and their customers interact. Yet, over the past 36 months, these assumptions have been challenged at an increasing rate. Emerging in their place is a new model characterized by a shift toward cloud computing, growth in the “Internet of Things,” and the rise of the software-defined network.

## This Is Now

### Great Cloud Migration Continues. Enterprise IT Dissolves.

Today’s final “frontier” is no longer physical but rather logical. Massive cloud companies are building this frontier—optimizing one or more aspects of what was traditionally the purview of the Information Technology function. Using a service model, cloud providers are revolutionizing the way enterprises buy and use infrastructure, applications, and even specific features (such as Domain Name Resolution or Security).

These days, it’s nearly impossible to find a company that hasn’t “cloud-sourced” some aspect of its IT functions. In fact, many now rely solely on IT services delivered via the cloud. Among high-tech players—including Uber, Netflix, and Pinterest—the trend is to not even bother building an internal IT function. Instead, they compete through cloud service providers. The cloud migration is analogous to when manufacturing plants shifted from generating their own electricity, previously a necessity, to connecting to power generation grids that could afford appropriate levels of quality and continuity of service. Today’s enterprises are finding that the cost and speed advantages of cloud cannot be ignored.

What does this mean for information security professionals? It means that our old model of centralized control, internal policies, employee awareness, and internal process certifications (such as ISO 27001) are giving way to something dramatically different—an approach akin to the just-in-time inventory systems of modern-day factories. After all, who cares if only one cog of an overall machine is secure? Every cog needs to be secure—and working in tandem with all of the other cogs.

The bottom line: The CISO of the future may have no infrastructure, no internally developed correlated reports, and no employees to educate. Yet, that scenario is largely out of sync with the ways in which today’s practitioners are being developed.

“How do I see the Internet of Things complicating the cybersecurity landscape? It increases the attack surface, increases the sophistication of the attack itself, and complicates mitigation requirements.”

*Domenico Martini  
Network Manager  
SEAT Pagine Gialle*

## Internet of Things (IoT) Brings an End to Controlled Endpoints and Introduces Incredible New Threats

The popularity of the FitBit—a wearable, connected device for health management—illustrates another macro-trend: the push toward nearly ubiquitous connectedness. Already televisions, washing machines, and refrigerators are online. Moving forward, automobiles, billboards, restaurant tables, and homes will become increasingly “self-aware”—connecting to us and with us in new and profound ways.

The ability to connect to anywhere from almost anything will drive dramatic efficiencies in the way we work and live. Yet, this “Internet of Things” will also introduce new and tremendous risk and threats. For example, as cars start driving themselves, they will become hacking targets, creating very physical threats around who is “at the wheel.” In the realm of cyber-attacks, the army of tomorrow will not be people, but rather “bots” represented by devices. Today, most security professionals are worried about the Bring Your Own Device (BYOD) problem, in which a new, uncontrolled device enters a “secure” networking environment. In reality, the challenges around today’s BYOD phone or tablet will soon be supplanted by more complex issues surrounding connectivity from both fixed consumer devices and embedded industrial devices.

Over time, most security professionals will find that controlling employee endpoint devices with security hardware and software is no longer feasible economically, technically, or politically. Thus, endpoint security will eventually give way to “entryway” security—that is, conducting security inspection of all requests to and from an application that is meaningful to the company rather than the network itself. The shift from endpoint to entryway will prompt dramatic changes in security approach, requiring skilled practitioners to make the transition. Those who resist—clinging to yesterday’s business model—will likely deal their companies near-fatal blows in costs, culture, and speed to market.

How do you see the Internet of Things (IoT) complicating the cyber-attack landscape?

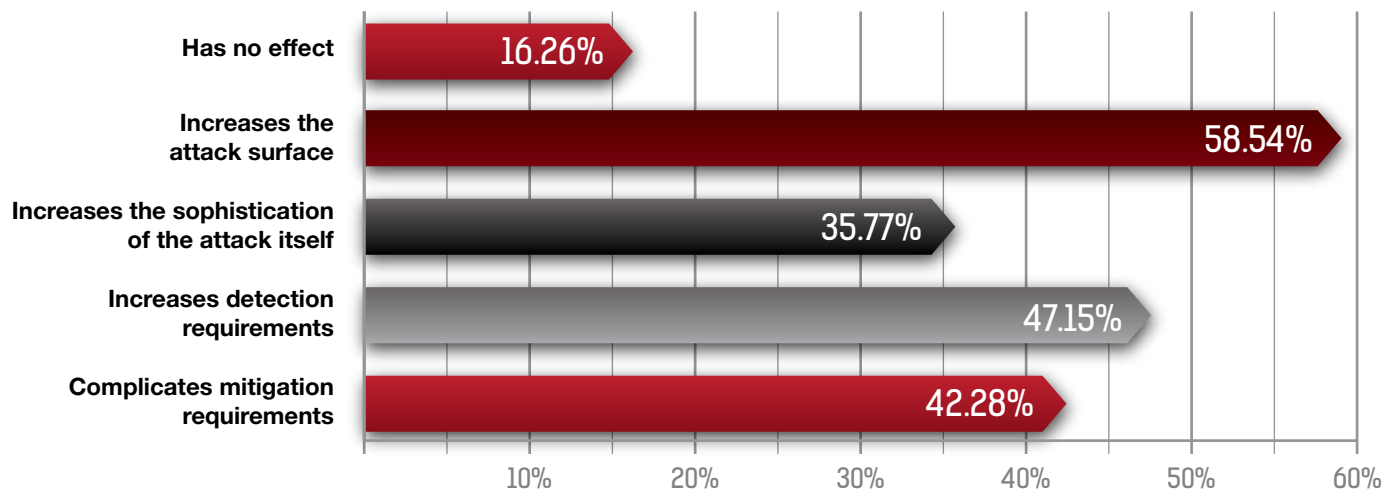


Figure 36: Internet of Things (IoT) in the cyber-attack landscape

## The Software-Defined Network Is Changing the Rules of the Game

If you have ever seen any of the Transformer movies, you can quickly grasp the idea of a software-defined network (SDN). In the blink of an eye, a device designed and architected to be one thing—a coffeemaker or automobile, for example—can be programmed and commandeered to do or be something else. The Transformers world combines the physical and logical aspects into one magical metamorphosis. While such change may not be realistic in the real world, the concept of logical transformation is quite real and already in use.



## How is your organization leveraging SDN?

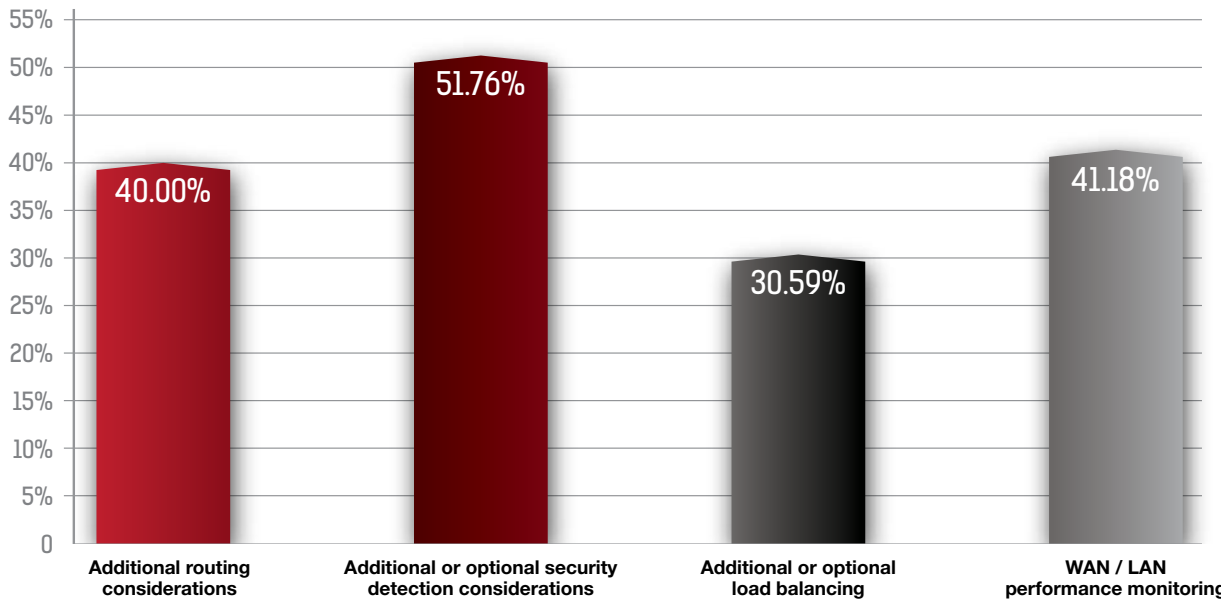


Figure 37: SDN use by organizations

SDN allows network administrators to manage network services by abstracting lower-level functionality—decoupling the system that makes decisions about where traffic is sent from the underlying systems that actually forward traffic to the chosen destination. Arguably one of the most promising and disruptive innovations of our generation, SDN is poised to upend how we leverage technology.

Two fundamental factors explain why billions of dollars will be made and lost during the adoption and departure phases of various SDN “killer apps.” First, SDN is principally built around the open-source concept OpenFlow, which makes it both vendor neutral and, in concept, free. Second, the features of SDN are incredibly compelling—allowing for large-scale network operation manageability and efficient use of networking gear to maximize hardware deployments and minimize over provisioning. Those capabilities overcome some of the most persistent challenges associated with traditional network designs, which were conceived before the idea of virtualization or cloud delivery models.

## In your opinion, what are the top security threats of SDN?

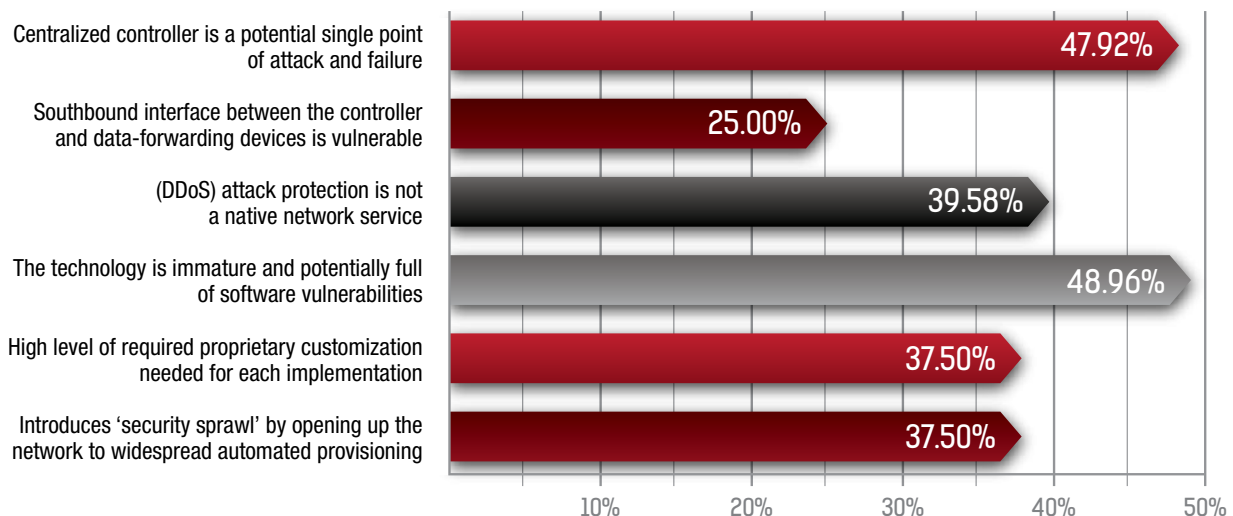


Figure 38: SDN security threats

"SDN DDoS capabilities are insufficient today and do not allow its customers to efficiently mitigate complex attacks. Granular data and metrics from our proprietary customizations also provide critical insights on attack vectors and drive quicker and more efficient remediation than SDN service providers."

*Julien Soriano*  
*Network Security Manager*  
*eBay*

In case you're harboring any doubts about SDN as an incredibly disruptive and immutable macro-trend, consider that Google advertises that it has built its entire network on SDN. The company does not buy network gear from any vendor. On cost alone, any carrier or cloud player that wants to compete with Google can't afford not to look into SDN operations.

Security professionals who don't understand the mechanics of SDN will be hamstrung. Blowing away the principle that inspected traffic must flow in certain ways, SDN can usurp modern-day security devices. Consequently, security professionals will face the need to protect information across unique and dynamic traffic routes. In addition, today's security inspection architecture lacks protections to the SDN control function—a crucial vulnerability. After all, if the SDN function is somehow compromised, this "mother ship" could wreak havoc across an entire environment.

## Get on Board

Whether or not you believe it, see it, or understand it, each of these trends has the ability to immeasurably change the information security landscape. And if all three trends materialize, the resulting changes will transform today's CISO role into the equivalent of a quaint, old-fashioned horse and buggy.

## Avoid obsolescence by getting started today:

- Begin the process of decommissioning endpoint protection investments. Migrate toward new "entryway" security investments, considering innovative ideas and technologies for "fingerprinting."
- Become obsessive about application security. Availability will be challenged as access comes from disparate devices and technologies via the Internet of Things.
- Prepare for large-volume attacks. Cyber-attacks will conscript consumer devices (not just phones) as well as industrial devices in attacks against you.
- SDN is already here. Attacks won't be far behind. Ask tough questions about SDN security: Are you ready? If not, how can you initiate a personal and professional project to close the gap? All the while, select security vendors wisely—avoiding those without an SDN strategy.



## About Boston Children's Hospital

- Ranked nationally in 10 pediatric specialties, with about 25,000 inpatient admissions each year and 557,000 visits scheduled annually through 200+ specialized clinical programs
- Experienced massive rate of several DDoS attacks from Anonymous—marking the first time a hacktivist group targeted a health care organization
- Seven other health care organizations that share the same ISP were affected, as well

## Anyone is a Target: DoS Attack Case Analysis on Boston Children's Hospital

Have we entered an era in which cyber-attacks can be not just disruptive and expensive but also potentially deadly? In 2014, Boston Children's Hospital (BCH) became the first health care organization to be targeted by a hacktivist group. Because BCH uses the same Internet Service Provider (ISP) as seven other area health care institutions, the organized attacks had the potential to bring down multiple pieces of Boston's critical infrastructure for health care.

While BCH and the other institutions survived the attack, their experiences should serve as a proverbial “shot in the arm” for any health care entity that isn’t already serious about security. To its credit, the medical community seems to have recognized the gravity of the situation. In fact, The New England Journal of Medicine—a publication normally focused on clinical studies—featured an article about the attacks authored by BCH’s CIO, Dr. Daniel Nigrin.<sup>1</sup>

The attacks on BCH have illustrated that information security is no longer simply the purview of the IT department. With health care now highly dependent on digital records and network connectivity, inability to access systems has potentially far-reaching clinical and business impacts. Dollars could be lost. Patient and staff safety could be compromised. Lives could be lost.

What follows is a review by Radware’s Emergency Response Team (ERT) as experienced from the front lines of the incident - and why it matters.

## The Attacks on BCH: A Timeline

Purportedly the work of hacktivist group “Anonymous,” the cyber-attacks launched against BCH—occurred in three major strikes launched:

### **Doxing<sup>2</sup>**

On March 20, 2014, BCH leaders received word of a threatening Twitter message that was attributed to Anonymous. The message relayed information related to a high-profile child-custody case, in which a 15-year-old girl with a complex diagnosis was taken into custody by Massachusetts protective services. The message threatened retaliation if the hospital did not take disciplinary action against certain clinicians and return the child to her parents. Attackers posted personal information—including home and work addresses, email addresses and phone numbers—of some of the individuals involved in the case. This activity is known as ‘doxing.’ By posting technical information about Boston Children’s website, the attackers also seemed to imply that the hospital’s external site might become a target.

### **DDoS Strike #1— Attacks at Relatively Low Rates**

Starting in early April, the attackers made good on their threats, targeting the hospital’s external website with a DDoS attack. At this point, the attack was relatively slow, yet visible to BCH IT personnel.

### **DDoS Strike #2— Attacks Ramp Up, Mitigation Deployed**

Over the course of a week, the attacks increased to the point that they slowed legitimate inbound and outbound traffic. This second string of attacks—comprised of DDoS attacks, scans and intrusion attempts—included TCP fragmented floods, out-of-state floods and DNS reflection floods (including UDP fragment floods). This also included the following non-DDoS attacks: UDP Scans, XSS, SQL-Injection and Directory traversal. At this point, mitigation was set in place and stopped the attacks from reaching the targeted servers.

### **DDoS Strike #3 — Attacks Peak with Round of Higher-Rate DDoS Attacks**

The third strike of the attack peaked at nearly 4x that of the second strike, reaching 28 Gbps. This time, the attackers also made multiple attempts to penetrate the hospital’s network through direct attacks on exposed ports and services. Additionally, the attackers used “spear phishing” emails. These emails tried to lure recipients into clicking embedded links or opening attachments, thereby granting access to a portion of the network behind the hospital’s firewall.

---

1 When ‘Hacktivists’ Target Your Hospital”, Daniel J. Nigrin, M.D., The New England Journal of Medicine 2014; 371:393-395

2 Document tracing, or “doxing,” is the practice of using the Internet to research and then share personally identifiable information about a subject.

Have you experienced severe slowness to your application with an inexplicable steep increase in traffic volume?

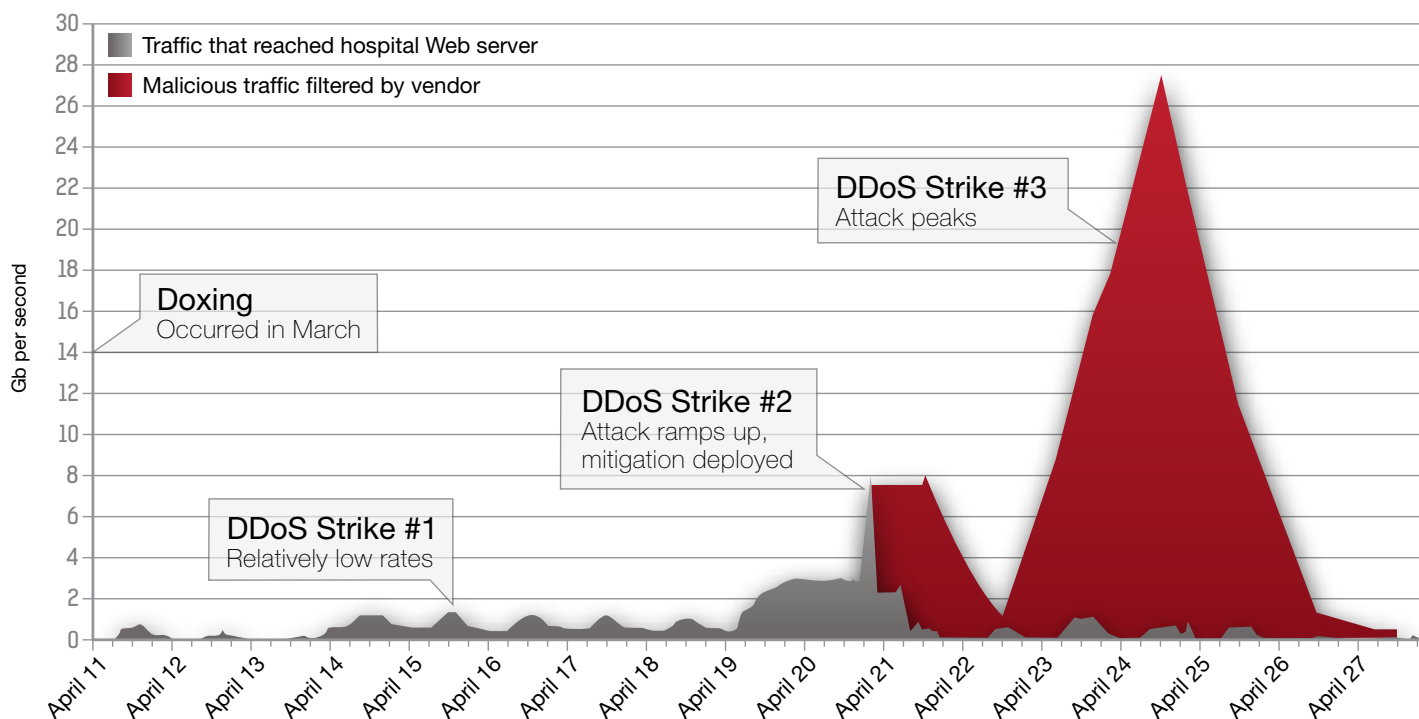


Figure 39: Internet traffic during DDoS Attack - The New England Journal of Medicine

## The Response

As soon as it became aware of the initial threat, Boston Children’s Hospital activated its multi-disciplinary incident response team. The team faced critical questions and decisions from a business, clinical and technical perspective.

From a business and clinical perspective, the team had to quickly assess what services would be compromised or lost if the hospital were to lose Internet connectivity. Significantly, the hospital had not conducted such an assessment prior to the attacks. In short order, the team identified three critical potential impacts:

- Inability to route prescriptions electronically to pharmacies
- Email downtime for departments where email supports critical processes
- Inability to access remotely hosted electronic health records (EHRs)

From a technical perspective, the BCH team invoked Radware’s ERT and the Radware scrubbing center due to the massive rate of several of the DDoS attacks. Because BCH shares an ISP with other hospitals, seven other health care institutions—Massachusetts General Hospital, Beth Israel Deaconess Medical Center, Dana-Farber Cancer Institute, Joslin Diabetes, Harvard Medical School and Harvard School of Public Health—also faced potential impact to their network and operations.

“In clinical settings, {cyber} attacks can clearly have adverse effects on patient care. Healthcare organizations should strongly consider investing the time and resources in IT security systems and operational best practices to ensure that they are prepared to ensure and defend against these new threats, if and when they occur.”

*Daniel J. Nigrin, MD*

*“When ‘Hacktivists’ Target Your Hospital”, Daniel J. Nigrin, M.D., The New England Journal of Medicine 2014; 371:393-395  
The New England Journal of Medicine*

## Lessons Learned

The DDoS attacks against Boston Children’s Hospital are not significant because of their technical sophistication. Rather, they are significant because they demonstrate that anyone—including health care entities—can be a target for cyber-attacks.

As Dr. Nigrin subsequently wrote in *The New England Journal of Medicine*, “In clinical settings, such attacks can clearly have adverse effects on patient care. Healthcare organizations should strongly consider investing the time and resources in IT security systems and operational best practices to ensure that they are prepared to ensure and defend against these new threats, if and when they occur.”

The attacks on BCH also serve as a reminder that even an organization that has taken all the “right” technical steps can still become a victim. Further, just as health care entities must constantly stay ahead of tenacious infections, all organizations must ensure continual vigilance about information security. It’s not enough to have a plan; it must be communicated well and updated constantly as threats and risks evolve.

That kind of vigilance becomes all the more important because of the potential for a massive “domino effect” across Boston’s critical infrastructure. Had the DDoS attacks been successful, they could have affected not only BCH but also seven other hospitals. That could have put care delivery—and patients’ lives—in peril.

## Pay Up or Else: IT Infrastructure Solutions Provider Helps Customers Navigate Range of Network Attacks

We live in a managed services world—with organizations across industries outsourcing significant pieces of their operations to third-party specialists. The business case for managed services can be compelling. But as cyber-security threats rise, so have the stakes for managed services providers. These companies must not only protect their own networks and data; they must also be effective guardians on behalf of their customers and their customers' customers.

As an IT infrastructure solutions provider, ServerCentral fulfills those dual roles of securing itself and its customers. The Chicago-based firm routinely identifies network and DDoS attacks, which occur as frequently as every few days and range from small protocol floods through full-blown DDoS campaigns designed to extort money in return for stopping the attack. In fact, earlier this year, one of the company's clients was the target of an organized criminal effort that involved attempted extortion.

The ServerCentral client, which offers a web-based tool for project management, was one of a number of victims of the same criminal group. This group's MO is simple: it threatens to attack a network if an organization does not meet its demands for payment.

After refusing to negotiate with the criminals, the ServerCentral client was hit with a 20GB DDoS attack. The incident underscores the important role that ServerCentral plays in its clients' network security. As Director of Network Engineering Ron Winward explains, "ServerCentral takes as much pride in our customers' ability to execute and offer service as we do in our own ability to provide infrastructure in support of mission-critical applications and business functions. We are equally focused on providing 100% uptime to their customers and end users."

### Detecting Extortion-Based Attacks

Winward explains that ServerCentral detects attacks in many different ways. In the case of the extortion-based attack, the customer notified ServerCentral of the threat.

"In some instances, customers will contact us, noting that something isn't right. They may recognize it as an attack or simply see something out of the ordinary," he says. "Attacks can also be detected by our network monitoring tools, which can identify anomalies and alert our Network Operations Center (NOC) of the incident."

## About ServerCentral

- IT infrastructure solutions provider specializing in the design, development and management of custom infrastructure solutions, including colocation, Infrastructure as a Service (IaaS), private clouds, network services and network protection
- ServerCentral customer was hit by an extortion-based DDoS attack
- Managed services providers need to remain vigilant in protecting their networks, as attacks can affect multiple customers—and all of their customers

ServerCentral engineering staff also regularly reviews network reporting data and can perform forensic research using historical flow analysis when needed. For customers that use Radware's DefensePro and DefenseSSL, ServerCentral's NOC and engineering staff are notified of detected events in real time.

After years of experience operating a resilient, high-performance network, Winward says ServerCentral was prepared to support its client through the extortion-based DDoS attack. In fact, the company has established a security model that it can apply to customer interfaces upon turn up.

"As a result, most customers don't even know they're being attacked until ServerCentral's monitoring system detects it," Winward says.

"As we see more and more attacks of all types, we have an obligation to share this knowledge with our customers so that everyone can be as vigilant as possible. We know that attackers are focused on their 'job' 100% of the time. Staying abreast of changes in attack patterns, objectives and execution is something that must remain 'on' at all times."

*Ron Winward  
Director of Network  
Engineering,  
ServerCentral*

## Planning for the Future

Groups responsible for many attacks—especially those that incorporate extortion—have a habit of stopping and starting an attack at random intervals. In other words, the attack could very well start up again at any time. Winward asserts that ServerCentral's core network architecture, deployment of carrier-class routers and forensic toolset help ensure that it's ready for even the most unpredictable attacks.

"We're able to quickly and easily manage the presence of an attack with a known or identifiable fingerprint," he says. "Offering DefensePro as a real-time option for individual customers further strengthens our position, especially for application-layer and SSL attacks."

He explains that the company keeps standby units on-site for rapid deployment, if needed—but acknowledges that the real-time responsiveness of DefensePro simply outmatches any reactive technique, no matter how fast it may be.

As attacks become both more sophisticated and seemingly easier to execute, Winward says that ServerCentral expects the number of attacks to double over the next 12 months. With that in mind, customer education is an increasingly important component of the company's strategy for attack management. ServerCentral is actively working to inform its customers about the risks—and steps they should take to proactively guard against them.

"As we see more and more attacks of all types, we have an obligation to share this knowledge with our customers so that everyone can be as vigilant as possible," he explains. "We know that attackers are focused on their 'job' 100% of the time. For ServerCentral, staying abreast of changes in attack patterns, objectives and execution is something that must remain 'on' at all times, as well."





# 09 | Executive Insights— From the Corner Office

Complementing our ongoing quantitative research, this year Radware launched our inaugural qualitative study to explore the most pressing problems and persistent challenges facing senior information security and technology executives around the globe.

Targeting CIOs, CISOs and VP-level executives across a myriad of industries, our research reveals that while information security was once the purview of the IT department, it is now on the minds of C-suite executives and a board-level concern. This chapter also illuminates the security challenges and issues executives are wrestling with—and the opportunities they see ahead. More specifically, we probed on a number of questions:

- Is there anything special about your industry that would make you more at risk?
- Do you know how many times you have been attacked in the last 12 months?
- How has handling cyber security threats to your organization changed in the last five years?
- What are the best measures you've implemented in the last 12 months to handle the newest security threats and why?
- Which of today's biggest IT trends—Bring Your Own Device (BYOD), Cloud, the Internet of Things (IoT) and software defined networking (SDN)—do executives believe pose the most significant risk for their organizations?
- What keeps security executives up at night, and why?

- Are security threats now a CEO or board-level concern in your company?
- How do you expect the cyber threat landscape to evolve moving forward in the next 12 months?
- What measures are cross-industry executives planning to implement in the next 1-3 years?

The survey garnered responses from corner offices within billion-dollar enterprises across multiple industries—including financial services, government, healthcare, higher education, manufacturing, telecommunications and transportation—in every region around the globe. What follows are some of the most illuminating findings and insights.

## Industry-Specific Risks

We asked respondents about security threats or challenges affecting their industry—financial services, government, healthcare, higher education, manufacturing, telecommunications and transportation. A number of executives indicated that they do indeed face some specific risks because of the nature of their industry.

Radware’s quantitative research suggests that for the financial services industry, the likelihood of cyber-attacks has actually decreased over the past year. Even so, the financial services executives in our study still believe that by its very nature, their industry is high risk. One specifically mentioned the need for comprehensive endpoint management to safeguard financial services organizations.

Other executives echoed their challenges of safeguarding industry-specific information. Citing the core mission of any community college—“very open public access”—a higher education executive captured one of the central challenges for these institutions. Making educational facilities, information and other resources more accessible to more people can create or compound vulnerabilities around data privacy, particularly when it comes to student records. Similarly, the CIO of a large federal contractor and the Chief Information Security & Privacy Officer of a large health system pointed to the sensitive information—government and medical data, respectively—that they must steward. In both cases, these executives face complex regulations designed to ensure privacy and security of sensitive government and patient information. They also face daunting legal, financial and reputational consequences if their organizations are unable to safeguard the data in their care.

## Looking Back

We asked executives about how many attacks their organizations had experienced in the last 12 months. Healthcare and manufacturing executives conceded that they do not know how many times their organizations were successfully targeted. By contrast, their peers in the education, financial services, government, telecommunications and transportation industries told us they could quantify their attacks. They credited a number of tools—intrusion detection/protection systems, log files as well as metrics and analytics—with enabling their organizations to detect and quantify attacks.

“[The telecommunications] industry has seen a sharp rise in targeted DDoS attacks as well as malware targeting our primary service offering: mobile devices. We’ve observed many attempts to compromise large numbers of mobile devices in an effort to build a botnet to target our infrastructure and/or the infrastructure of another organization.”

*Dannie Combs  
CISM Senior Manager,  
Network Security  
U.S. Cellular*

For many executives, the past five years have brought significant change in how their organizations handle security threats. Security is no longer a “part-time job,” with most respondents indicating they now have teams dedicated to security. Several pointed to “exponential growth in volume [and] complexity” of attacks, along with greater awareness among senior leaders. A telecommunications executive noted that his company has quintupled investments, increased headcount and restructured the organization to better position security teams to proactively identify cyber security risks, mitigate attacks, conduct forensics and manage compliance obligations.

We also asked the executives to think about more recent changes: the best measures they have implemented over the past 12 months. Some of the responses reflected a change in communication and training, such as instituting daily review meetings and conducting user awareness training. Others pointed to new technical capabilities, including advanced analytics, intrusion/threat detection and monitoring, secure email, user access control, web browser content filtering and desktop sandbox security.

According to Dannie Combs of U.S. Cellular, the company has increased headcount and added redundancy to critical security infrastructure. In addition, U.S. Cellular has added new security tools to further enable deep visibility and forensics capabilities—driven primarily, he says, by “the reality that the attack volumes, complexities and frequency have increased year over year.” Meanwhile, an executive for a global player serving government clients reporting separating internal systems from BYOD devices in order to limit entry points for threat vectors. A manufacturing executive indicated that his company has implemented ShareFile to improve the way it controls data.

## Trendy—and Risky?

We also asked the executives about Bring Your Own Device (BYOD), cloud computing, the Internet of Things (IoT) and software-defined networking (SDN)—four of the most powerful macro-trends shaping the information security landscape.

As use of smart phones, tablets and other mobile devices has surged, so has the prevalence of BYOD in the enterprise. BYOD offers a number of potential benefits to an organization but can also introduce new and complex risks. At the same time, organizations across sectors are continuing the great migration to the cloud, suggesting that the end of traditional enterprise IT may not be far in the future.

Two other innovative trends—the Internet of Things and the SDN—have also emerged. The Internet of Things has arisen from the growing prevalence of connected devices—not just computers or smart phones, but also consumer devices (such as major appliances and automobiles) and embedded industrial devices. This growing connectedness may prompt the end of endpoint security and the dawn of entryway security. SDN—which decouples the system that makes decisions about where traffic is sent from the underlying systems that actually forward traffic to the chosen destination—is poised to upend the way networks are managed and secured. In our survey, cloud and BYOD—the two more established trends—were cited by more than one-third of executives who believe they increase security risks for their organizations. The Internet of Things was selected by more than a quarter of executives, while less than one-fifth cited the SDN.

## Losing Sleep in the C-Suite

- Financial Services – “I only know what I know.”
- Education – “Breach of personally identifiable information and records.”
- Healthcare – “Detecting attacks. [We] cannot do it.”
- Telecommunications – Higher volume and frequency of attacks. “An attack 30 to 40Gbs per second, or larger, would cause an immediate impact to our business.”
- Manufacturing – “Inability to prevent internal threats. Users continue to trust virus/malware emails.”
- Government Contractor – “Breach of personal information—the cost and impact to company name.”

## Losing Sleep: What’s Keeping Executives Up at Night?

We also wanted to know what’s causing cross-industry executives to lose sleep. What are the risks, threats and trends they consider most worrisome? Even within an industry, responses varied widely, but a number voiced concerns about their inability to detect attacks; “I only know what I know,” as a VP of a major financial institution noted. The Chief Information Security & Privacy Officer of a large hospital pointed to attack detection, admitting that the hospital simply cannot do it. Internal threats—whether borne of malice or ignorance—remain a chief concern for the Chief Technology & Information Officer of a global manufacturer.

For the Vice Chancellor of IT at a college, breach of personally identifiable information and records was the top concern—reiterating the challenge of keeping data secure in an environment designed to foster easy access. A telecommunications executive articulated his fears around growing volume and frequency of attacks. “An attack 30 to 40Gbs per second, or larger, would cause an immediate impact to our business.” And a government contractor’s CIO told us he’s most worried about breach of personal information and the resulting cost and reputational impact on the firm.

## Looking Ahead

Nearly three-quarters of executives told us that security threats are now a CEO or board-level concern. Some mentioned negative press coverage as the impetus for greater focus on threats. Others pointed to the potential impact on the business—as well as the need for increased funding and the growing liability associated with cyber-attacks and other threats. In the hospital’s C-suite, executives have taken note of the American Hospital Association’s documentation regarding what boards and CEOs should know about information security.

Given this growing emphasis on security, we also wanted to know the executives’ thoughts about the future, including specific plans for the upcoming year. When we asked whether respondents expected more attacks, fewer attacks or about the same volume, the response was unanimous: “Expect more attacks.”

When thinking of future plans, analytics and big data emerged as themes—underscoring the growing importance of increased security intelligence. A healthcare executive cited plans to implement FairWarning®, while a peer from the financial services industry noted application whitelisting—that is, letting only known programs run—as among his organization’s upcoming plans.



This section looks at the 2014 business and attack trends and provides a set of best practices for organizations to consider when planning for cyber-attacks in 2015.

## Recap: C.H.E.W. – Motivation, Capability & Intent

In considering best practices, four types of security threats (C.H.E.W.) remain top of mind:

- ⚠️ Cybercrime** – Criminal attacks are typically motivated by money. Large in number and present in virtually every country around the globe, these groups range in skill level from basic to advanced.
- 👥 Hacktivism** – Hacktivists are primarily motivated not by money but rather by a desire to protest or seek revenge against an entity. As with criminals, there are a large number of hacktivist groups. However, most of these groups have basic skills. A few “standout” individuals possess advanced skills and motivate a potentially larger set of followers.
- 👁️ Espionage** – These attacks are aimed at acquiring secrets to support national security, to obtain economic benefit or both. A growing number of countries have the ability to use cyber-attacks for espionage—and a larger array of groups is being “supported” or “tolerated” with such activities.
- 🚀 War (Cyber)** – The fourth, and arguably most nefarious, type of attack: those motivated by a desire to destroy, degrade or deny. A growing number of countries have the ability to use this form of “politics by other means.” Further, non-state actors seem poised to undertake cyber-attacks as a form of war.

## Cyber-Attack Defense = Attack Detection + Attack Mitigation

At its core, cyber-attack defense has two components: detection and mitigation. As illustrated in Figure 40, success hinges on both the quality and time of detection and mitigation.

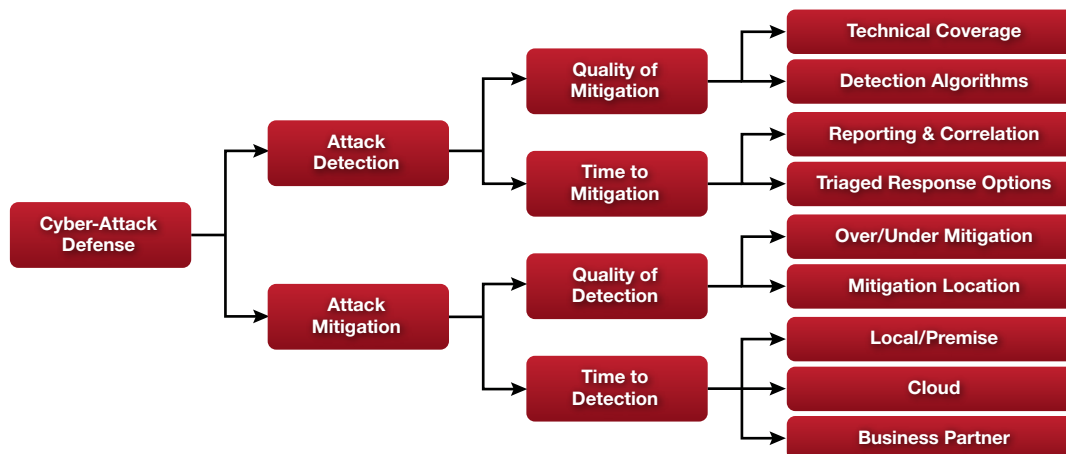


Figure 40: Cyber-Attack Defense = Attack Detection + Attack Mitigation

## How to Evaluate a Vendor for DDoS & Cyber-Attack Mitigation

When evaluating a vendor for DDoS and cyber-attack mitigation, examine capabilities and strengths in the two core competencies: detection and mitigation. Assess each vendor against these criteria—aiming to maximize capabilities in each of these areas.

How good is the vendor at detection?

**Quality – This section evaluates the ability for the vendor to provide high-quality detection:**

Type(s) of Detection Available

- Netflow
- Openflow
- Packet L3/4
- Packet L7 Header Required
- Packet L7 Headerless
- Coverage of OWASP Vulnerabilities
- Inputs/Signals from Other Mitigation Tools

Deployment Model Options

- In-Line
- OOP – Synchronous
- Hybrid Cloud Options
- Internal Scrubbing Center – Asynchronous
- Cloud Scrubbing Center – Asynchronous
- Software Defined Networking (SDN)
- Virtual Deployment Options
- Feeds from Partners/Works with Other Vendors' Signals

**Time – This section evaluates the categories required for modern attack detection:**

- Real-Time Options
- Signaling/Automatic Options (for Advanced Application Attacks)
- Signaling/Automatic Options (for Cloud Diversion)

**Reporting & Response – This section evaluates the categories required for controlling and reporting modern attack detection:**

- Real Time
- Historical
- Forensics
- Intelligence Reporting (that is, can detect before attack)
- Detection Support Response – Real Time
- Detection Support Response – On-Site Options
- Integrated Reporting with Cloud Portal
- Ability to Discern Legitimate vs. Illegitimate Traffic in Real Time

## How good is the vendor at mitigation?

**Quality – Does the vendor over-mitigate or under-mitigate the threats? How many technologies are leveraged to assist?**

- Rate-Only
- Routing Techniques
- Rate Behavior Only
- Other Than Rate Behavior
- Heuristic Behavior
- Statistical Behavior
- Signatures – Static with Update Service
- Signatures – Custom Real Time
- HTTP Server-Based Protections
- HTTP OWASP-Based Protections
- Hybrid Signaling/Cloud Scrubbing Center Coordination
- SSL Protections
- HTTP Redirects
- JavaScript Challenge & Response
- Cloud Challenge Response

**Time – How quickly can the vendor begin mitigation?**

- Real-Time Options
- Automatic Options

**Reporting & Response – How granular is the reporting? Can a user see if legitimate traffic is being impeded by the mitigation technique?**

- Real-Time Displays
- Historical Mitigation Effectiveness Measures
- Forensics & Detail Reports
- Emergency Response Options
- Displays Legitimate & Illegitimate Traffic
- Displays All Attacking Vectors Granularly
- Mitigation Response Attack-Back Options
- Mitigation Support Response – Real Time
- Mitigation Support Response – On-Site Options
- Integrated Reporting with Cloud Portal

## Summary of Best Practices

When planning cyber-attack defense, be mindful of the C.H.E.W. threats, be demanding of vendors and always consider the following tenets:

### **Timing is everything.**

Organizations need to look at time to mitigate as a key success factor. With that in mind, 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 not just one attack vector, but also 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.**

With 2015 upon us, SSL attacks remain a major threat. 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.

# 11 | Summary—The Fearful Five



## The Fearful Five

As security professionals, many of us speak passionately about attack vectors, cyber-incidents or trends in information security. Just as often, we are asked to share our opinions on what we find most frightening and how businesses, governments and individuals can mitigate those risks. In reflecting back on 2014 — and looking ahead to 2015 — we at Radware are focused on five critical concerns.

- 1 Attacks That Kill**  
For years, we've seen demonstrations of how attacks on all sorts of things—pacemakers, trains, automobiles and even aircraft systems—could one day lead to loss of life. Today, there's no doubt that cyber-attacks can and will turn deadly. It's no longer a question of "if" but "when."
- 2 Reduced Sense of Urgency**  
Even as media reports and public awareness are at all-time highs, a certain sense of apathy or fatigue seems to have settled in among security decision makers. Perhaps many have grown disheartened and numb, believing that in the face of



persistent attackers, a sense of urgency and doing the right thing will ultimately prove futile. At Radware, we fear that business executives are increasingly abandoning rigorous exploration of how to secure endpoints and other points more effectively. We suspect that such execs are succumbing to the idea that becoming a victim—if they haven't already—is simply a foregone conclusion.

### 3 More Critical Infrastructure Outages

It's not hard to imagine how widespread cyber-attack disruptions could cripple a nation's critical infrastructure services—including power generation, water supply, cellular, telephone or television delivery services, or even police and first-responder networks. Even the world's most advanced countries are not immune to this.

### 4 Rise in Cyber Hostage-Taking

While there is a long history of cyber ransom activity, 2014 brought a new level of threat in criminal attacks. Nefarious groups have begun taking digital assets or services hostage—commandeering these resources until certain demands, which may or may not be financial, are met. In at least one case, this hostage-taking has led to business failure.

### 5 Mass Adoption of Cyber-Attack Laws, Including Nationalistic Rules

We believe that as government faces an increasingly dissatisfied, frustrated constituency—as well as growing threats around state-sponsored espionage—legislators will begin the process of writing laws on cyber-attacks. Such laws will likely aim to dictate network traffic flows, security levels at critical infrastructure companies and acceptable data processing domiciles. They will also provide guidelines on what constitutes acceptable Internet behavior.



## 12

In September and October of 2014, Radware conducted a survey of the security community and collected 330 responses. The survey was sent to a wide variety of organizations globally and was designed to collect objective, vendor-neutral information about issues organizations faced while planning for and combating cyber-attacks. All responder profile information is listed below. Please note that not all answers add up to 100%, as some responders may have skipped the question.

Which of the following best describes you and your role at work?

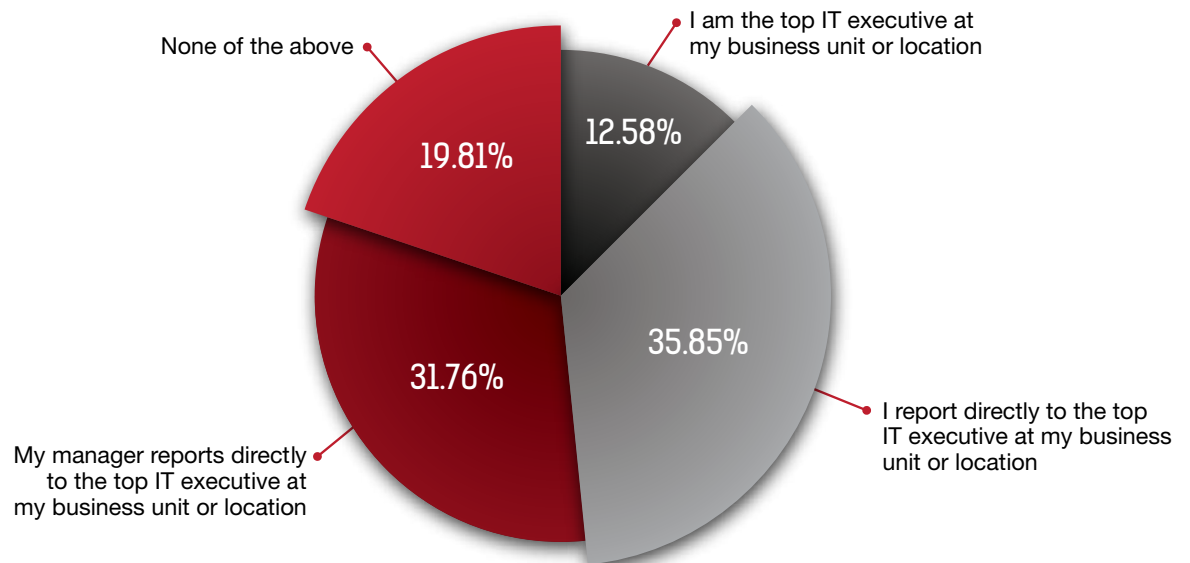


Figure 41: Role within organization

Which of the following best describes your title within your organization?

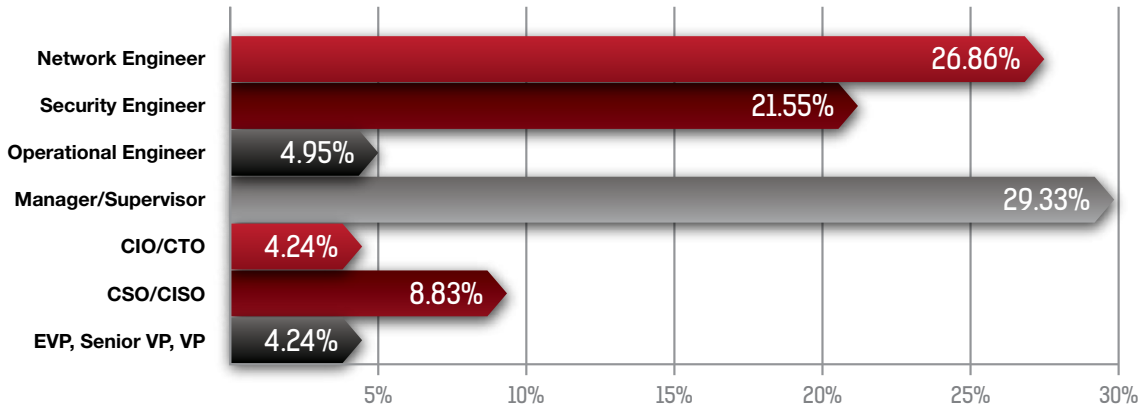


Figure 42: Title within organization

What is your organization's total global annual sales revenue for the most recent fiscal year?

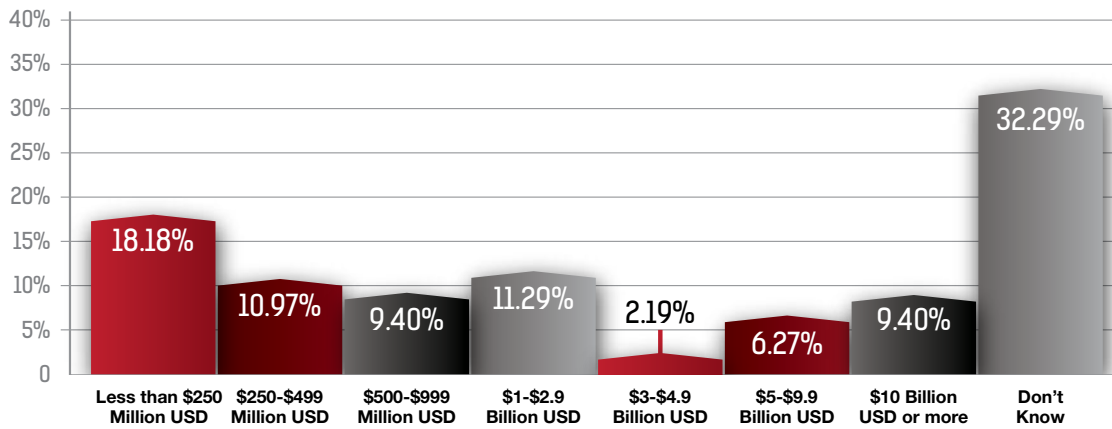


Figure 43: Annual revenue

How many employees are currently working in your organization?

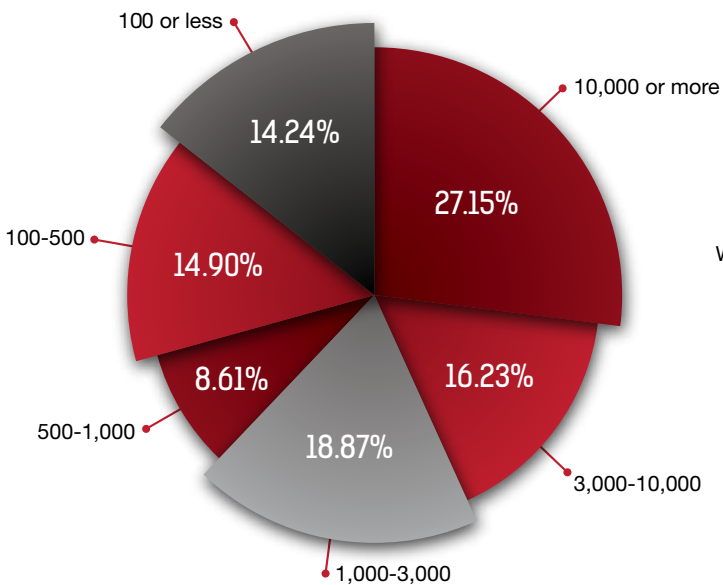


Figure 44: Number of employees in the organization

What is the scope of your organization's business?

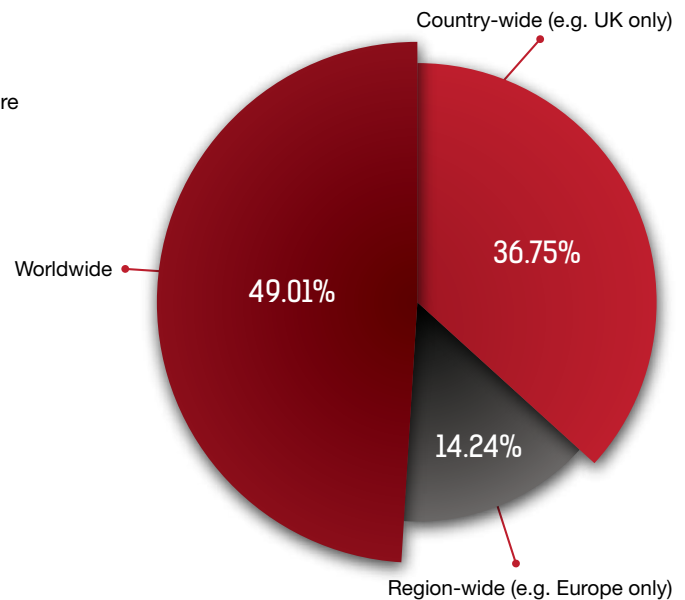


Figure 45: Geographic scope of business

## Which of the following best describes your company's industry or function?

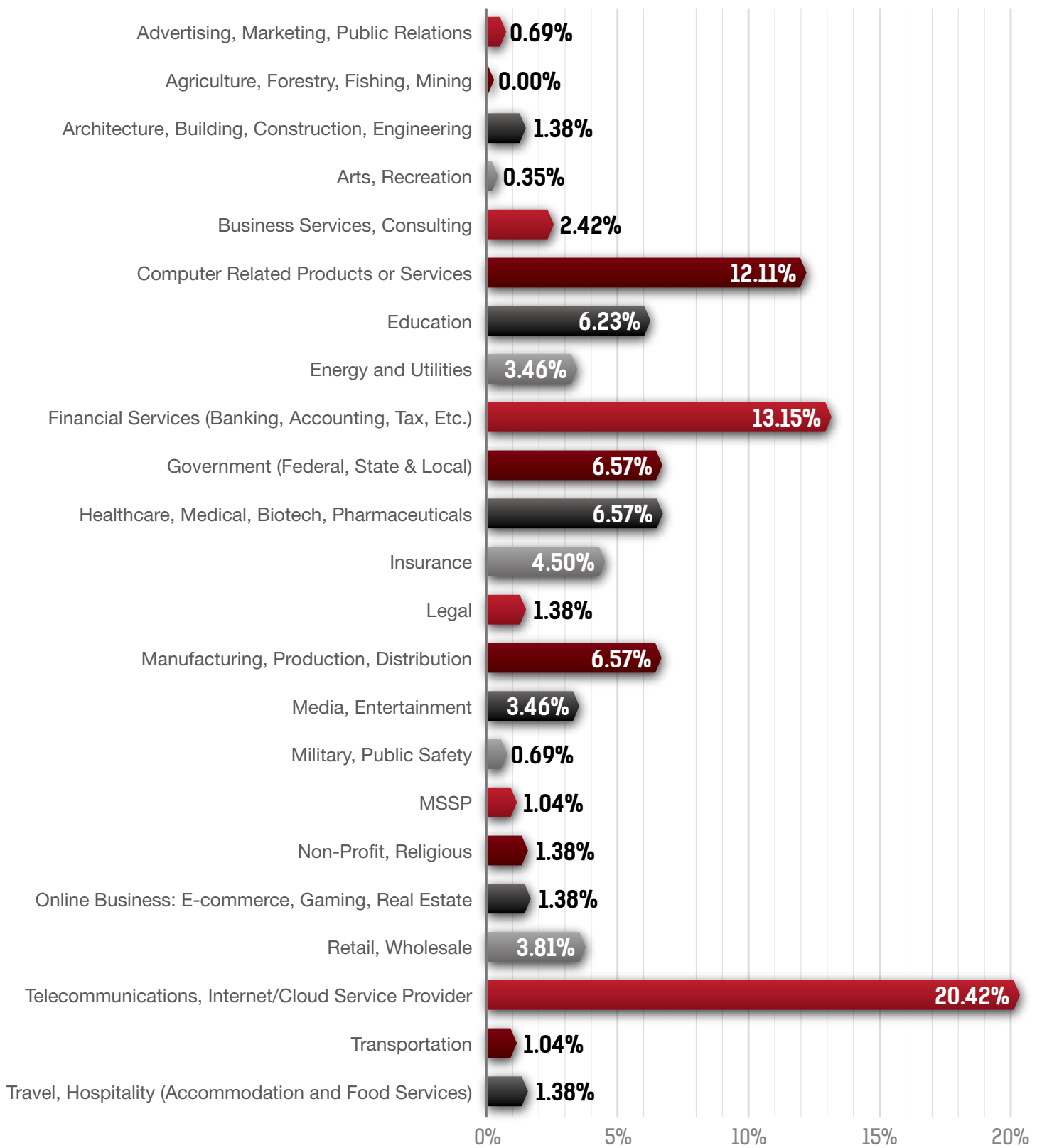


Figure 46: Industry

## Authors

Carl Herberger  
*VP Security Solutions*  
Radware

Ziv Gadot  
*ERT Consultant*  
Radware

Yotam Ben-Ezra  
*Director of Security Product Management*  
Radware

Oren Ofer  
*Senior Security Researcher*  
Radware

## Advisory Board

Werner Thalmeier  
*Director of Security Solutions*  
Radware

Alon Lelcuk  
*VP Security*  
Radware

Dudi Lavi  
*Director of Security ERT*  
Radware

Shira Sagiv  
*Security Product Marketing Director*  
Radware

## Special Thanks

Carolyn Muzyka  
*Director, Marketing Communications*  
Radware

## About the Authors

Radware (NASDAQ: RDWR), is a global leader of **application delivery** and **application & network security solutions** for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit [www.radware.com](http://www.radware.com).

## About the Radware Emergency Response Team (ERT)

Radware's ERT is a group of dedicated security consultants who are available around the clock. As literal "first responders" to cyber-attacks, Radware's ERT members gained their extensive experience by successfully dealing with some of the industry's most notable hacking episodes, providing the knowledge and expertise to mitigate the kind of attack a business's security team may never have handled.

## For More Information

Please visit [www.radware.com](http://www.radware.com) for additional expert resources and information and our security center [DDoSWarriors.com](http://DDoSWarriors.com) that provides a comprehensive analysis on DDoS attack tools, trends and threats.

Radware encourages you to join our community and follow us on: [Facebook](#), [Google+](#), [LinkedIn](#), [Radware Blog](#), [SlideShare](#), [Twitter](#), [YouTube](#), [Radware Connect](#) app for iPhone®



© 2014 Radware, Ltd. All Rights Reserved.  
Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.

[www.radware.com](http://www.radware.com)