Help Net Security
January 16, 2019

The costs of cyberattacks increased 52% to $1.1 million

Radware has released its 2018-2019 Global Application and Network Security Report, in which survey respondents estimate the average cost of a cyberattack at $1.1M. For those organizations that calculate (versus estimate) the cost of an attack, that number increases to $1.67M.

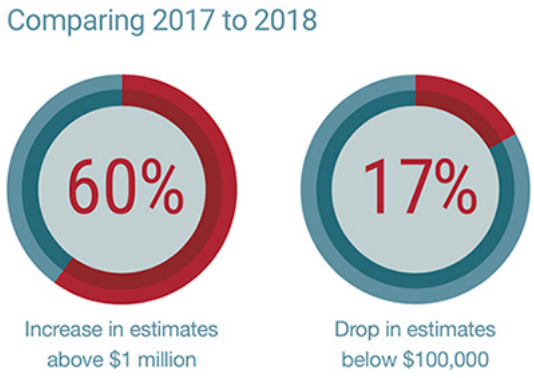
		REGION			
Have Experienced a Cyberattack in Past Year	Total	USA/Canada	APAC	EMEA	CALA
Financial/ransom	51%	52%	48%	61%	43%
Political/hacktivism/social	31%	27%	30%	32%	37%
Insider threat	27%	28%	29%	22%	30%
Competition/espionage	26%	26%	28%	29%	20%
Cyberwar/geopolitical conflict related	18%	22%	17%	21%	12%
Angry users	18%	20%	12%	19%	23%
Motive unknown/other	31%	36%	30%	32%	24%
Have not experienced any cyberattacks	2%	2%	2%	4%	1%

Motives for cyberattacks on organizations vary by region

The top impact of cyberattacks, as reported by respondents, is operational/productivity loss (54%), followed by negative customer experience (43%). What's more, almost half (45%) reported that the goal of the attacks they suffered was service disruption. Another third (35%) said the goal was data theft.

While the cost of attack mitigation continues to rise, so does the number of organizations under attack. Most organizations have experienced some type of attack within the course of a year, with only 7% of respondents claiming not to have experienced an attack at all. Twenty one percent reported daily attacks, representing a significant rise from 13% last year.

Not only are attacks becoming more frequent, they are also more effective: 78% of respondents hit by a cyberattack experienced service degradation or a complete outage, compared to 68% last year. Even with these numbers, 34% of respondents do not have a cybersecurity emergency response plan in place.



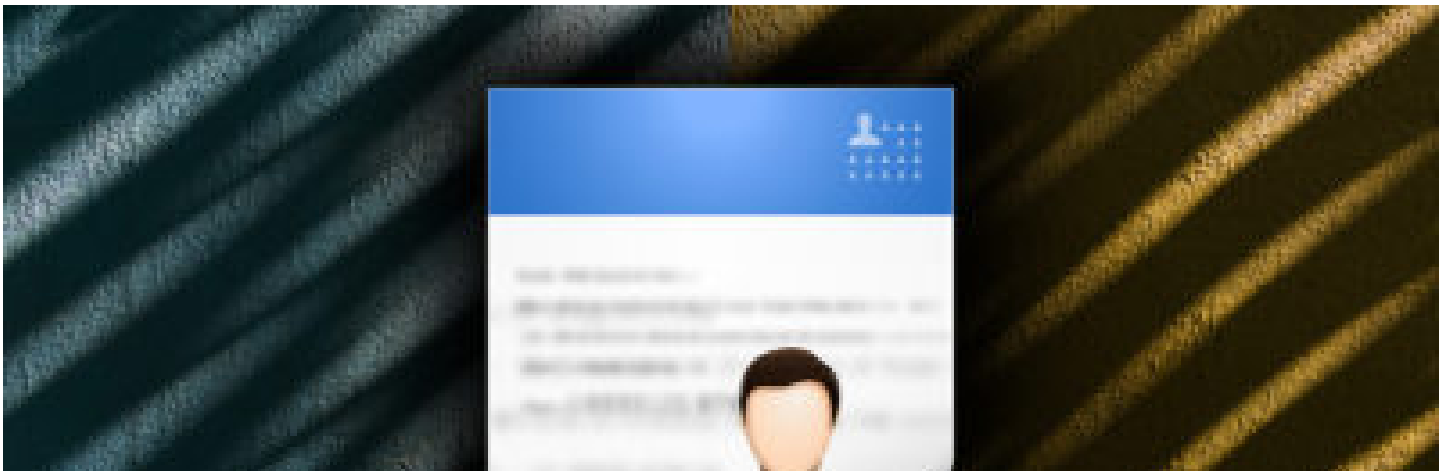
Companies' estimates of costs related to cyberattacks are on the rise

Other key findings of the report include:

- 43% of respondents reported negative customer experiences and reputation loss following a successful attack.
- Data leakage and information loss remain the biggest concern to more than one-third (35%) of businesses, followed by service outages.
- Hackers increased their usage of emerging attack vectors to bring down networks and data centers: Respondents reporting HTTPS Floods grew from 28% to 34%, reports of DNS grew from 33% to 38%, reports of burst attacks grew from 42% to 49%, and reports of bot attacks grew from 69% to 76%.
- Application-layer attacks cause considerable damage. Two-thirds of respondents experienced application-layer DoS attacks and34% foresee application vulnerabilities being a major concern in the coming year. More than half (56%) reported making changes and updates to their public-facing applications monthly, while the rest made updates more frequently, driving the need for automated security.
- 86% percent of surveyed businesses indicated they explored machine-learning (ML) and artificial intelligence (AI) solutions. Almost half (48%) point at quicker response times and better security as primary drivers to explore ML-based solutions.

More about cybersecurity Radware survey

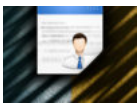
Share this article



0patch releases micropatch for Windows Contacts RCE zero-day
Cybercrime could cost companies trillions over the next five years
Researchers analyze DDoS attacks as coordinated gang activities
Mining malware evades agent-based cloud security solutions
Compromised ad company serves Magecart skimming code to hundreds of websites

Spot light **Beware the man in the cloud: How to protect against a new breed of cyberattack**

What's New



0patch releases micropatch for Windows Contacts RCE zero-day

SSDP amplification attacks rose 639%

Agents of disruption: Four testing topics argue the case for agentless security

Industry reactions to Google's €50 million GDPR violation fine

Business resilience should be a core company strategy, so why are businesses struggling to take action?

Microsoft launches Azure DevOps bug bounty program

Machine learning trumps AI for security analysts

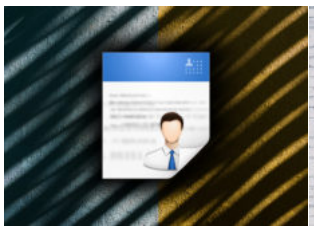
Bug in widespread Wi-Fi chipset firmware can lead to zero-click code execution

Companies still struggle to detect IoT device breaches

The costs of cyberattacks increased 52% to $1.1 million

BEC scammers add payroll diversion to their repertoire

Don't miss



0patch releases micropatch for Windows Contacts RCE zero-day

Industry reactions to Google's €50 million GDPR violation fine

Business resilience should be a core company strategy, so why are businesses struggling to take action?

Agents of disruption: Four testing topics argue the case for agentless security

SSDP amplifi rose 639%

Newsletters

Subscribe to get regular updates from Help Net Security. The weekly newsletter contains a selection of the best stories, while the daily newsletter highlights all the latest headlines!

Your email address

Weekly newsletter Daily newsletter

subscri

Start
News
Malware
Articles
Reviews
Events

Search

Read our privacy policy
About us
Advertise
Design by FatDUX