



CYBERCRIME BY THE NUMBERS

Malware, ransomware, data breaches, and phishing are top of mind for most companies. But what are the realities of falling prey to a cyberattack?

SCALE

70%

of organizations have had a security incident that negatively impacted their business in the past year.¹



84%

of enterprises have suffered phishing attacks.²



390,000

Over **390,000** new malicious programs are registered every day.³



93%

of phishing emails are related to ransomware.⁴



980

DATA BREACHES

In 2016, there were **980** data breaches with more than **35 million records** exposed.⁵



91%

of cyberattacks and the resulting data breach begin with a phishing attack.⁶



CryptoWall version 4, a notorious ransomware virus, has so far resulted in \$18 million in damages, **36,000+** confirmed victims, and **7.1 million** attempted infections.⁷



VULNERABILITY

The average network security breach goes undetected for over 5-8 months.⁸

201

DAYS

Mean time to identify a data breach is **201 days**.⁹



19%

Less than **19%** of data breaches are self-detected.¹⁰



38%

Only **38%** of global organizations feel prepared for a sophisticated cyberattack.¹¹



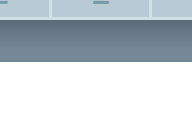
IoT

80%

MOBILE APPS

71%

80% of IoT and 71% of mobile applications are not tested for security vulnerabilities.¹²



25%

of companies do not treat cyber threats as significant corporate risks.¹³

COST

\$6

TRILLION

Global cost of cybercrime is predicted to hit **\$6 trillion** annually by **2021**.¹⁴



\$1.68

The estimated cost of using existing cloud offerings to break into most Wi-Fi networks is **\$1.68**. It would take **six minutes**.¹⁵



68%

of funds lost as a result of a cyberattack were declared unrecoverable.¹⁶



\$18

MILLION

Average cost of an **APT data breach is \$18 million**; **50%** is damage to brand reputation.¹⁷



68%

of corporations have not considered the **financial impact** of a cyberattack.¹⁸



The Internet economy annually generates between **\$2 trillion and \$3 trillion**. It's estimated that cybercrime extracts between **15% and 20%** of that value.¹⁹



Most organizations fold their security budgets and spending into another cost center, whether **IT (48%), general operations (19%), or compliance (4%)**, where security budget and cost line items are combined with other related factors. Only **23%** track security budgets and costs as its own cost center.²⁰



SUMMARY

- The rate of evolution and volume of complex targeted threats continue to increase.
- The growing prevalence of mobile, cloud, hybrid WANs, direct Internet access, and IoT is only going to exacerbate this problem.
- Existing security point solutions and applications are often reactive, inconsistent, and ineffective.
- The consequences of not proactively preparing for a targeted attack are enormous.

Companies need real-time visibility into the threats that could impact their network.



Once a threat is identified, companies need a simple, fast, and convenient method of mitigating these attacks.



SOLUTION

READ "5 MUST-ASK DNS QUESTIONS" AND VISIT AKAMAI.COM/ETP TO LEARN MORE.

SOURCES

- RSA Cybersecurity Poverty Index 2016, <https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016>
- <https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/>
- <https://www.av-test.org/en/statistics/malware/>
- <http://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html>
- Identity Theft Resource Center: 2016 Data Breach Category Summary, <http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2016.pdf>
- 2016 Enterprise Phishing Susceptibility and Resiliency Report, <https://phishme.com/2016-enterprise-phishing-susceptibility-report/>
- <https://cyberthreatalliance.org/pr/pr-092616.html>
- Mandiant M-Trends Report 2015, <https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf>
- 2016 Ponemon Institute Cost of Data Breach Study, <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SELO3094WWEN>
- InfoCyte: The Breach Detection Gap and Strategies to Close It, <https://www.infocyte.com/breach-detection-gap-conf>
- ISACA 2015 Global Cybersecurity Status Report, http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf
- Arxan: 2017 Study on Mobile and Internet of Things Application Security, <https://www.arxan.com/2017-Ponemon-Mobile-IoT-Study>
- MMC Cyber Handbook 2016, http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf
- Cybersecurity Ventures: 2016 Cybercrime Report, <http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016>
- <https://www.technologyreview.com/s/425770/the-criminal-cloud>
- <https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety>
- Ponemon Institute - The Economic Impact of Advanced Persistent Threats, <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN>
- MMC Cyber Handbook 2016, http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf
- McAfee Net Losses: Estimating the Global Cost of Cybercrime, <https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>
- SANS Institute: IT Security Spending trends, <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>

