CYBERARK®

REPORT

CYBERARK GLOBAL ADVANCED THREAT LANDSCAPE REPORT 2018: THE BUSINESS VIEW OF SECURITY

Examining the alignment gap and dangerous disconnects between business and security leaders

www.cyberark.com

Table of Contents

About the CyberArk Global Advanced Threat Landscape Report 2018

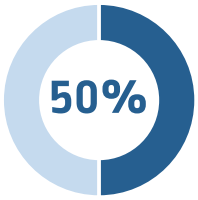
The CyberArk Global Advanced Threat Landscape Report 2018 is the 11th of its kind and will be released in three parts. The survey was conducted by Vanson Bourne in fall 2017 amongst more than 1,300 IT security decision-makers, DevOps and app developer professionals and line of business owners, across seven countries worldwide.

The business view of security: examining the alignment gap and dangerous disconnects

What do business leaders make of security? How do they perceive its practice and importance? Where are the gaps between business and security leaders? Part two of the CyberArk Global Advanced Threat Landscape Report 2018 explores these issues via responses from individuals including IT security decision-makers and line of business owners, from organizations ranging in size from 500 employees to 5,000 or more workers.

Security builds trust – but trust can be betrayed

Customers and partners expect to be notified when their information is compromised. So it was particularly striking to find a lack of transparency about data breaches. Half (50%) of respondents say their organizations did not fully inform customers when their personal data was compromised in a cyber attack.



Half (50%) of respondents

say their organizations did not fully inform customers when their personal data was compromised in a cyber attack.

Summary

Greater investments in cloud, DevOps and automation are supporting the growth of digital businesses. These investments are also expanding the attack surface, creating greater security risks across the organization and leading to the need for increased oversight, legislation and accountability. More than ever, cyber security is a shared problem, no longer solely the remit of the security team.

Survey results found that, despite widespread concern about cyber security among line of business owners, adoption of security best practices remain glaringly absent. While there are areas of alignment with security IT leaders, gaps with line of business owners associated with cyber security awareness are unnecessarily exposing organizations to serious risks and could impact their organization's ability to effectively identify and respond to a breach.

With the EU's General Data Protection Regulation (GDPR) data privacy law becoming a reality in 2018 amid heightened expectations for transparency and rapid breach notification requirements, alignment between business and security teams will take on a greater sense of urgency.

The implications of this lack of transparency are significant, including potential loss of future customers, executive departures and regulatory penalties that are evolving in severity.

This behavior also suggests that recent high-profile examples of similar actions by companies such as Yahoo! and Uber[1] are only the tip of the iceberg. In the case of Uber, the company tried to cover a data loss involving 57 million passengers and drivers in October 2016. The data from the survey also reinforces that, despite these headline-generating breaches, organizations are not changing fundamental security behavior.

In many industries, businesses are required by state, federal and international law to report breaches of personal information to affected customers. In the U.S., 48 states have statutes that require businesses and government agencies to notify customers of data loss. The U.S. does not have a single comprehensive federal law on data breach notification, but several federal statues require reporting, including the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach Bliley.

The EU's GDPR data privacy law becomes enforceable on May 25, 2018. GDPR is a major piece of legislation that will impact organizations around the world. GDPR replaces a much older regulation, the Data Protection Directive (Directive 95/46EC), which was adopted more than 20 years ago. GDPR includes comprehensive rules designed to harmonize data privacy laws and protect the personal data rights of any persons residing within the EU. It also includes breach notification requirements and a controller who must inform regulators of a data breach within 72 hours of discovery. Failure to do so may mean being penalized up to €20M or 4% of annual global revenue, whichever is the greater. In Australia, the Notifiable Data Breaches scheme, due to commence in 2018, establishes a mandatory data breach notification requirement and Singapore's Personal Data Protection Commission (PDPC) Guide to Managing Data Breaches directs that it is good practice to notify individuals affected by a data breach.

Executives are a prime target and security best practices are lacking

It was reassuring to see that security professionals understand that no organization is safe from increasingly complex, targeted cyber security attacks. In fact, security professionals believe that a cyber security compromise has a very good chance of affecting their organization, with nearly half (46%) saying their organization can't stop every attempt to break into their internal network. Interestingly, confidence is on the wane: when we asked the same question in last year's survey, 75% had a degree of confidence that they could prevent an attack.

46% of security professionals say their organization can't stop every attempt to break into their internal network.

Further, 58% of IT security professionals say that their organization is susceptible to carefully crafted attacks - like phishing attempts that target a company executive. Similarly, 63% of line of business owners agree that their organization is susceptible to this kind of compromise.

Unmanaged, unsecured third-party and remote vendor access remains a significant security risk. More than half (51%) of all survey respondents reported that they give third-party vendors remote access to their internal networks and, of this group, 23% fail to monitor remote vendor activity.

[1] https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Much more concerning is that lax security practices remain rampant across global organizations, with many employees still engaging in practices that introduce further risk. For example, 42% of business leader respondents say they store passwords in a document on a company PC or laptop, and 21% record credentials in a (paper) notebook or store them in a filing cabinet. Additionally, 31% of security professionals surveyed still do not use a privileged account security solution to store and manage privileged and/or administrative passwords. These respondents also reporting using very insecure methods as well, with 36% storing passwords in a document or spreadsheet on a company PC or laptop, and 19% keeping credentials in a notebook or filing cabinet.

There are well-publicized examples of this kind of sub-optimal practice making headlines. In December 2017, a number of United Kingdom Members of Parliament admitted sharing passwords with fellow workers, contravening Parliament's cyber security policy.[2]

Business leaders work to balance security awareness and personal responsibility

Considering that mounting risks and regulations have made cyber security a critical business requirement, it's troubling that many line of business respondents report a lack of security awareness. In fact, nearly half (49%) of line of business owners say they do not have adequate knowledge of their organization's security policies. Surprisingly, the security professionals we surveyed did not have much more confidence in what are presumably their own policies; a third (33%) said they did not have adequate knowledge.

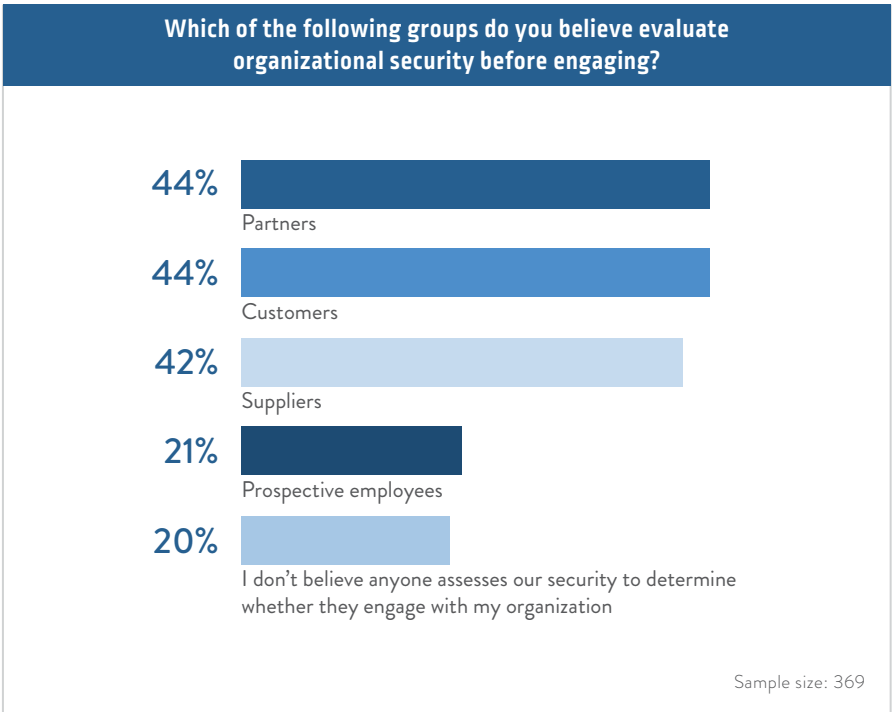
Further adding to the evidence of a knowledge gap, more than half (52%) of business leaders also do not understand what they should do if a cyber security incident occurs. Perhaps this lack of overall understanding accounts for these seemingly counter-intuitive findings: 75% of line of business owners say their CEO and/or board provides sound leadership for cyber security strategy. Taken in tandem with the fact that 82% of line of business owners say they are concerned about introducing an attack by (for instance) inadvertently clicking on a phishing mail, this may indicate that business leaders are confident in general about security but, when it gets to brass tacks, are unsure what to do in specific situations.

The security ecosystem

The consequences of compromise are not lost on those individuals and companies that form part of an organizational ecosystem, with 44% of line of business owners saying potential partners assess their organization's security before doing business with them.

The same percentage of business respondents (44%) say potential customers also consider security in advance and, from our entire respondent base, less than one-fifth (17%) believe that security doesn't matter to their potential customers. The expectation appears to be, then, that sensitive data will be protected by vendors and service providers. Clearly, that isn't always the case.

[2] http://www.bbc.co.uk/news/technology-42225214



Line of business owner respondents only. Multiple responses permitted.

In conclusion, optimism can be found in the fact that the business leaders we surveyed believe that their company's executive leadership should take a more proactive role in cyber security awareness, with more than three-quarters (78%) opining that security should be discussed at the board level more frequently. Top-down leadership is a must to solve the issues discussed in this report; senior figures must take responsibility and be accountable for cyber security within organizations of all kinds if the awareness gap we face is to be effectively addressed with more robust and widely understood security policies.

Download the first report in the series: CyberArk Advanced Threat Landscape Report 2018: Focus on DevOps.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in privileged account security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blog or follow on Twitter via @CyberArk, LinkedIn or Facebook.