Check Point
SOFTWARE TECHNOLOGIES LTD.

CLOUD • MOBILE • THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

ACHIEVING FIFTH GENERATION CYBER SECURITY

A Survey Research Report of IT and Security Professionals

MARCH 2018

INTRODUCTION

The pursuit of the highest level of cyber security is a top priority for IT and Security professionals worldwide. Check Point Software's latest worldwide survey research aims to shed light into these concerns and means for overcoming them by asking IT and Security professionals to walk us through their security posture pre and post cyber-attacks. The survey was conducted among 443 IT and Security professionals worldwide during January-February of 2018.

EXECUTIVE SUMMARY

- **The primary barriers** IT and security professionals declare as standing between their organization and high level cyber security effectiveness are: Staffing challenges (mentioned by 70% of IT and Security professionals), security conflict with business or user experience (56%), and outdated security infrastructure (50%). In staffing issues security professionals are referring to low numbers of cyber security staff as well as lack of staff knowledge needed to fight 2018 cyber-crime. When it comes to outdated security, security professionals are mentioning outdated security architecture as well as controls.

- **96% of organizations use various pre-attack preparation tactics**. Three main activities mentioned by Security professionals are timely patching (53%), search for attack trends (45%), and end-user security campaigns inside the organization (44%).

  Nonetheless, **security professionals still do not feel prepared enough**, rating their organizations as only moderately prepared for cyber-attacks (3.56 on a 1-5 readiness scale).

- **41% of organizations faced at least one cyber-attack during 2017**, with an average of **56 attacks per organization per year**.

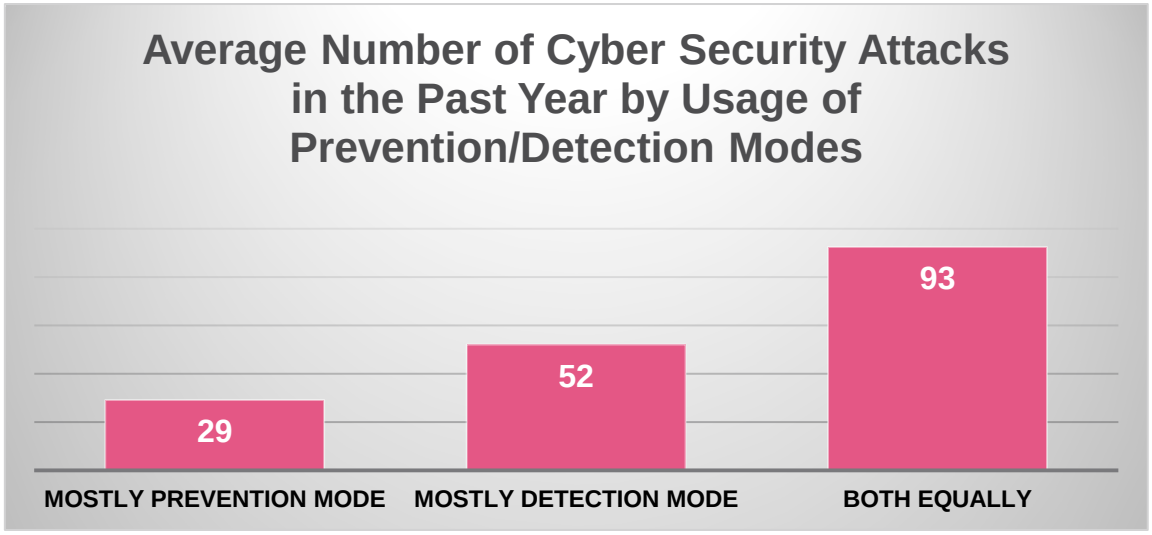
- **67%** of IT and Security professionals claim their organizations' **customers are inquiring which measures they are taking to protect their data.** This places IT Security professionals and cyber security strategy at an important fork of business junction. We predict this requirement will continue to grow once GDPR commences in May 2018.

HOW CAN IT AND SECURITY PROFESSIONALS BETTER PROTECT THEIR ORGANIZATIONS?

Our survey reveals barriers for higher level security cited by IT and Security professionals are merely the ones they are aware of. **The key lies in cyber security precautions security professionals are unaware of**: Prevention vs. detection mode, disparate point products vs. consolidated cyber security, and generation of security.

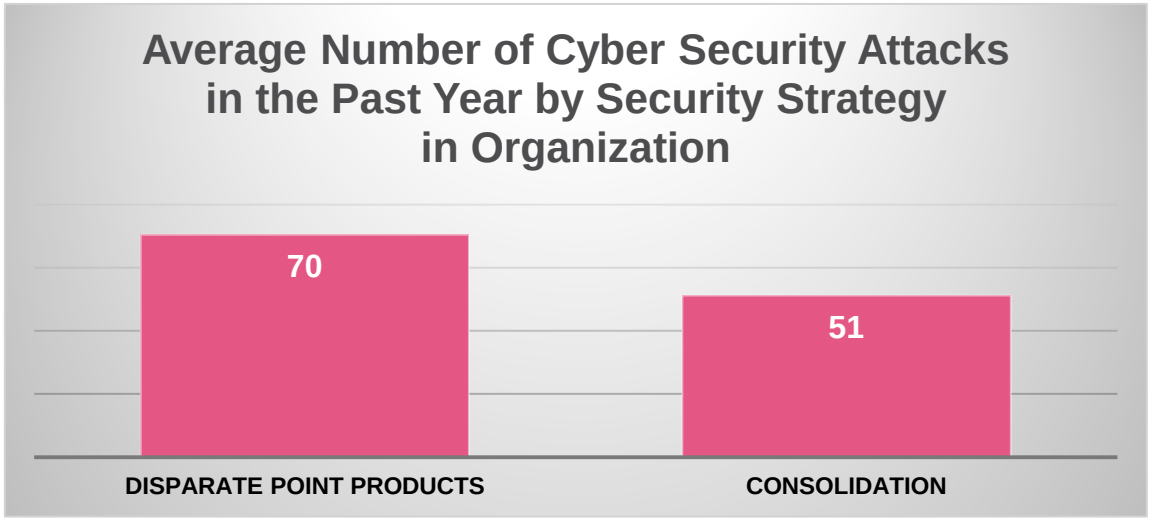
- **Prevention** (block attacks when detected) **vs. Detection security modes** (generate an alert indicating a breach was detected, without blocking it):

  Organizations who implement their security in detection mode faced 79% more cyber-attacks than organizations who implement their security in prevention mode (52 attacks in detection mode vs. 29 in prevention mode on average per year). Those who use mainly detection mode also experienced 27% more staffing challenges, in comparison to organizations who implement their security in detection mode.



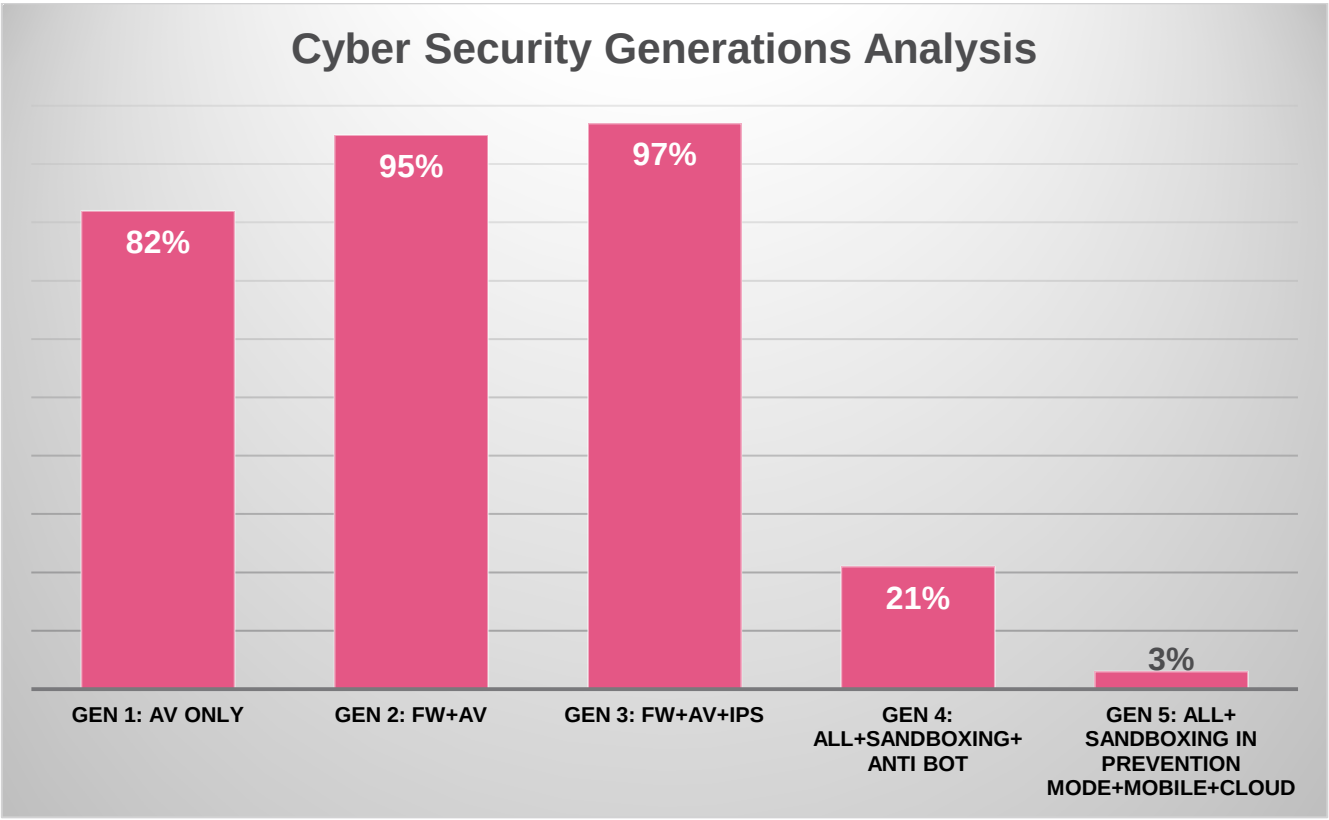
- **Consolidated security** (use a primary vendor for most security solutions) **vs. disparate point products** (aka 'point solution') **security strategy**:

  Organizations who apply disparate point products security strategy faced 37% more cyber-attacks than companies applying a consolidated security posture (70 vs. 51 attacks on average per year).



- **Generations of cyber security**:

  Our survey reveals outdated security is even more of a challenge than security professionals are aware of. When asked which cyber security solutions are used in their companies, one-fifth of organizations (21%) claim to use advanced threat prevention capabilities (aka Gen 4 cyber security). Only 3% are using threat prevention capabilities in prevention mode, and adding a layer of cloud and mobile security (aka Gen 5 cyber security). The rest are placing their organizations at risk for Generation 5 multi vector and mega-attacks.



RECOMMENDATION

The combination of security implementation in prevention mode as well as consolidated security strategy achieves the highest levels of security that is required against Gen 5 cyber-attacks.

For deeper analysis: See survey results detailed findings on pages 5-15.

Detailed Findings

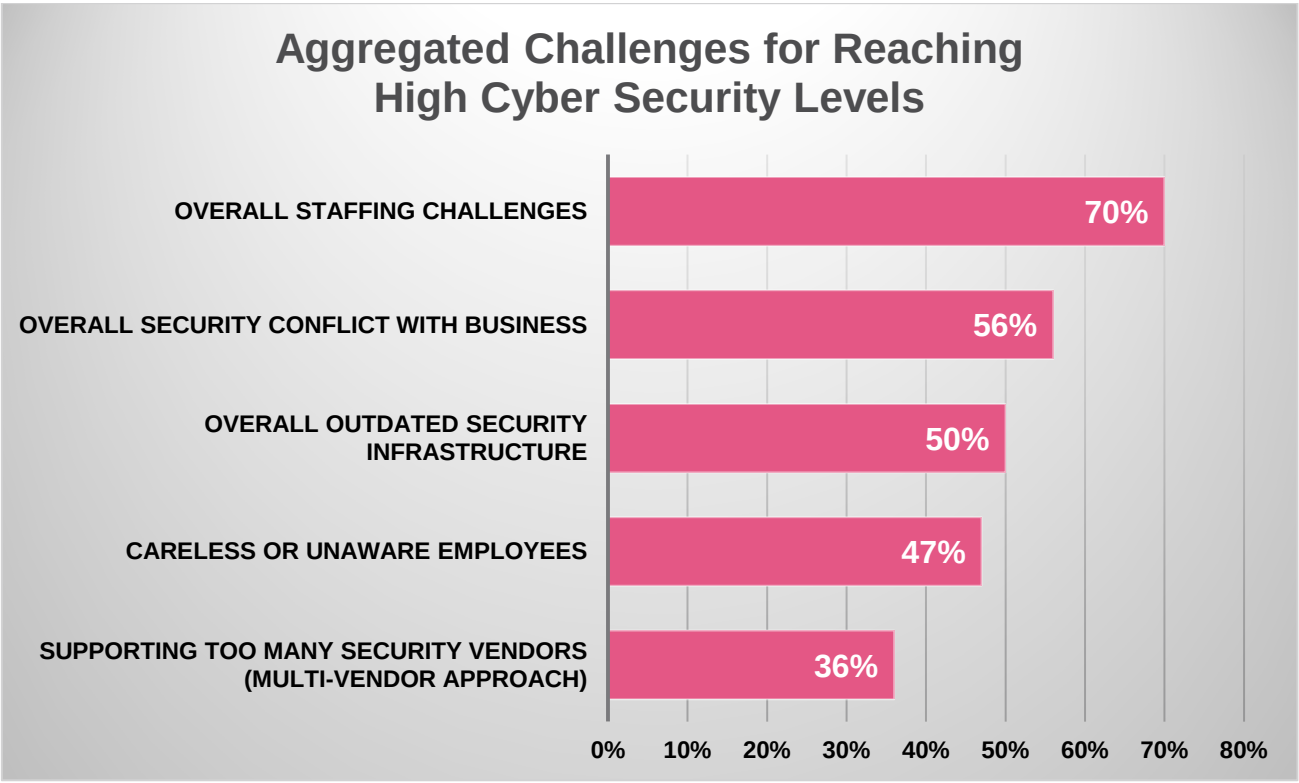
PERCEIVED OBSTACLES IN ACHIEVING HIGH SECURITY LEVELS

The main barriers IT and security professionals perceive as standing between their organization and high level cyber security effectiveness are: staffing challenges, security conflict with business, and outdated security infrastructure.

Cyber security teams strive for better and more effective security in their companies. Nonetheless, they report a wide range of obstacles in the way of achieving these goals. Most prominent obstacles mentioned are insufficient number of security staff (mentioned by 49% of IT and Security professionals), careless or unaware employees (47%) and security staff lacking the knowledge needed (44%).

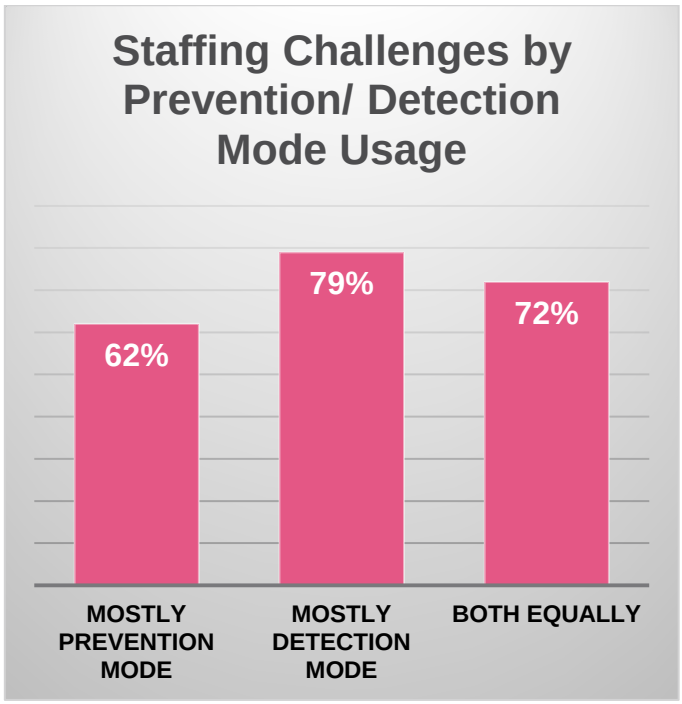
When aggregating obstacles categories, the three categories that rise as the most influential perceived obstacles are staffing challenges (70% of IT and Security professionals), security conflict with business (56%) and outdated security infrastructure (50%).

Staffing issues were mentioned more by the industrial vertical organizations. Companies from the healthcare industry mentioned security conflict with business and outdated security more than others.



Staffing issue: less of a challenge among companies using prevention mode and security consolidation strategy

The most prominent obstacle mentioned is the staffing challenge: quality and quantity of cyber security staff. This challenge is mentioned 27% more by organizations that implement detection mode vs. prevention mode. In addition, staffing challenges are mentioned 10% more by those applying a disparate security vendor's strategy (point solution) vs. a security consolidation strategy.



PRE-ATTACK PREPARATIONS

In preparation for a cyber-security attack, 96% of organizations use various tactics

Main data or actions applied in pre-attack preparations scenarios are: 53% of organizations conduct timely patching, 45% consume cyber-attacks trend articles, and 44% conduct end user security awareness campaigns. An additional 41% have risk assessment teams in-house.

Timely patching is conducted more in the financial, manufacturing and government industries (67%).

Only 23% have a pre-defined attack recovery playbook (slightly more among European companies, 28%).

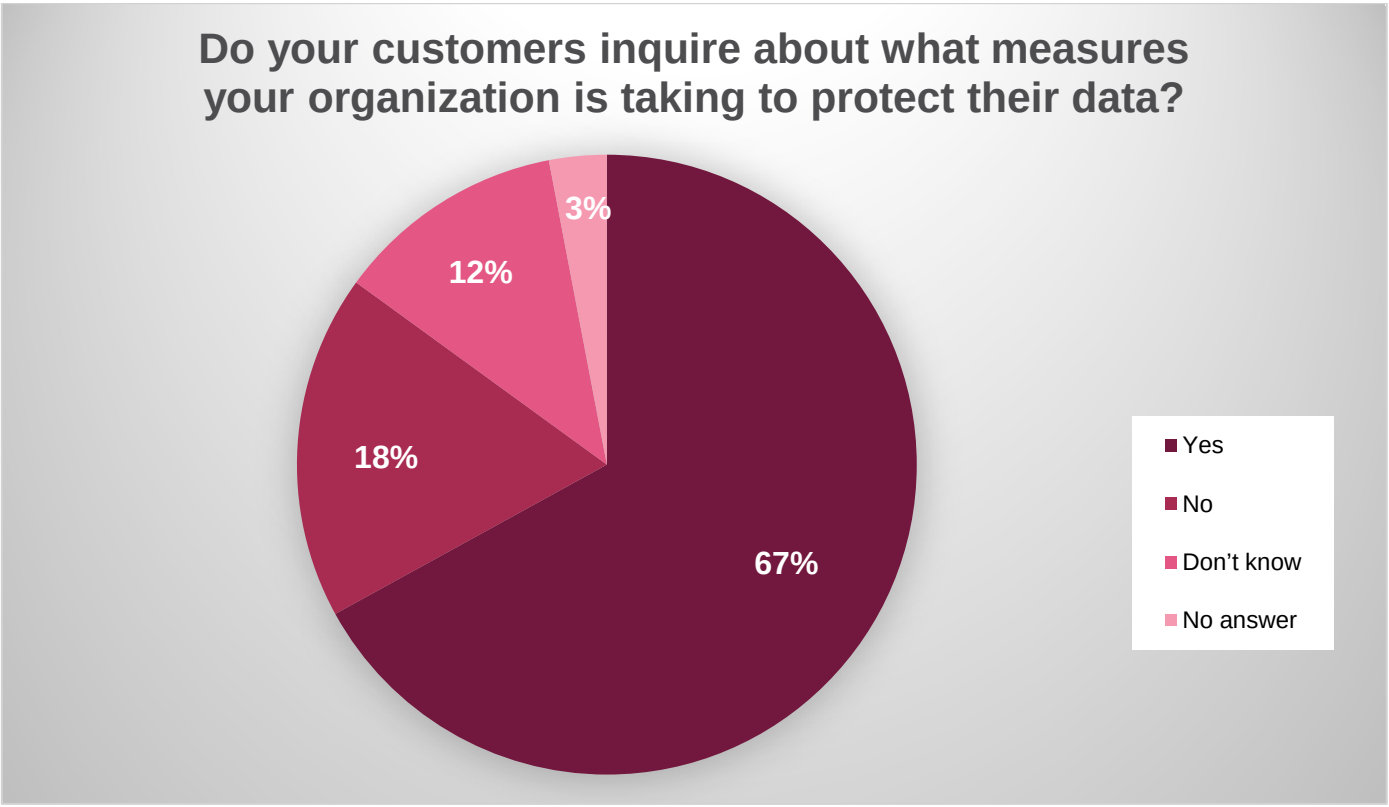
Although taking various precautions, only mediocre perception of pre-attack readiness.

IT and Security professionals were asked to rate their perception of pre-attack preparation readiness in their organization on a scale from 1-5 (1 being very poor to 5 excellent).

Overall, perception of pre-attack preparation level among IT and Security professionals is mediocre and stands at an average of 3.56.

67% of IT and Security professionals claim their organizations' customers are inquiring which measures they are taking to protect their data.

This places IT and Security professionals and cyber security strategy at an important fork of business junction.



CURRENT STATE OF CYBER SECURITY IN ORGANIZATIONS

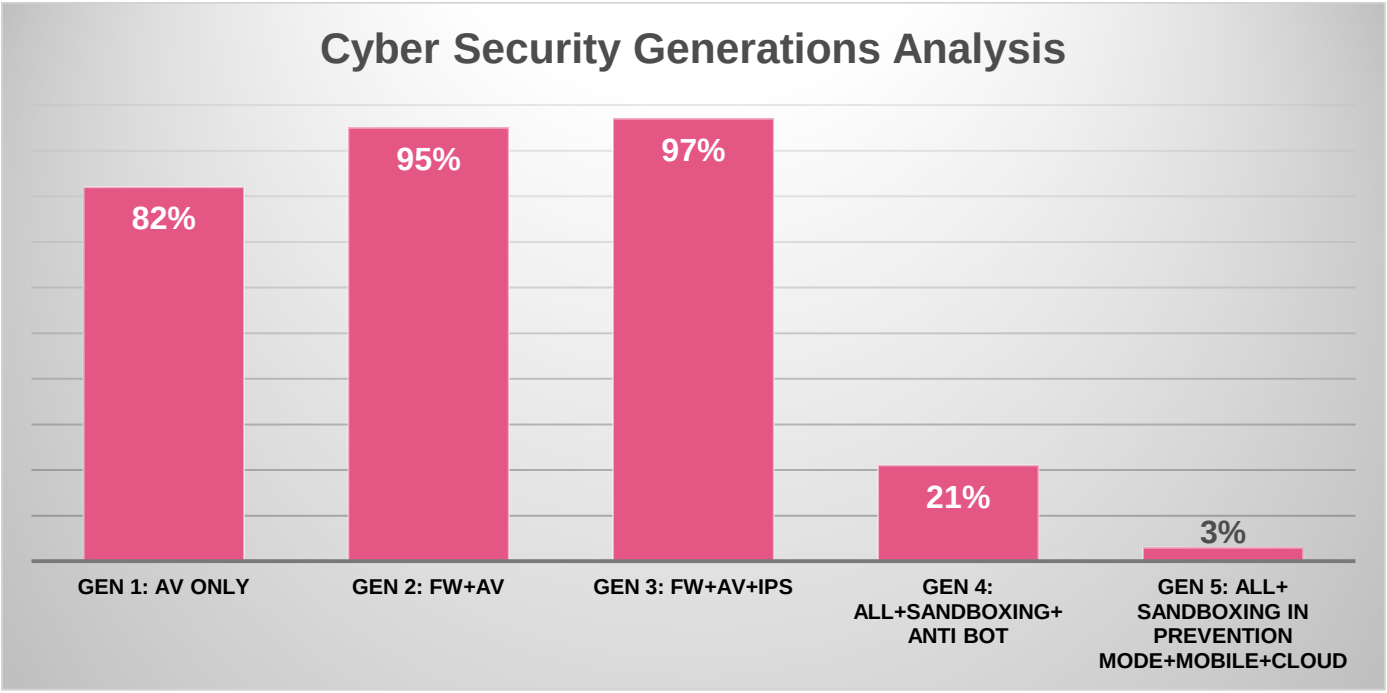
Only 3% of organizations are currently at Gen 5 Cyber Security Level.

IT and Security professionals in the survey were asked which cyber security solutions they use in their environment and what cyber security strategy is applied in their organization.

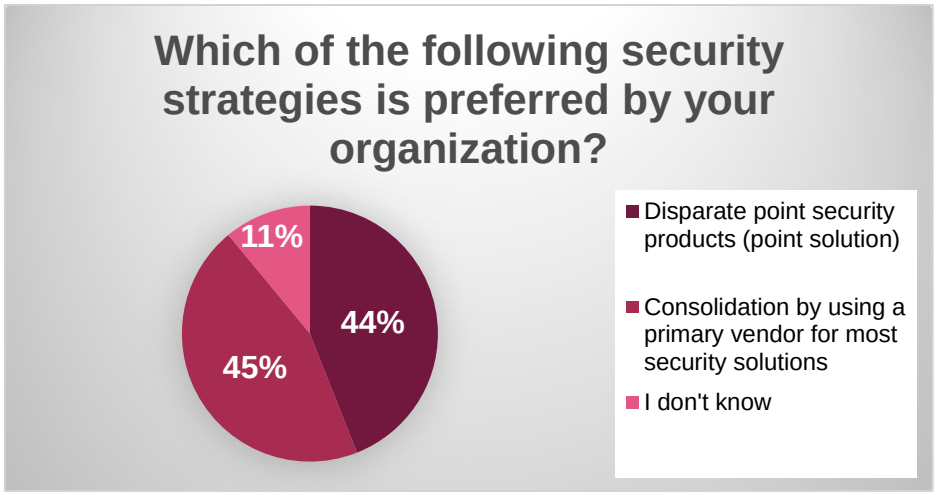
As a first and very important layer, our survey shows that Firewall, Antivirus and IPS are used by 97% of organizations (Generation 3 of cyber security solutions).

21% of those organizations also add additional layers of sandboxing and Anti-bot technology (Generation 4 of cyber security).

Only 3% of organizations add a layer of cloud security, mobile security and implement security technologies in prevention mode (block attacks when detected), as opposed to detection mode (generate an alert indicating a breach was detected, without blocking it). These 3% are securing their organizations at the highest level currently found- Generation 5 of security.



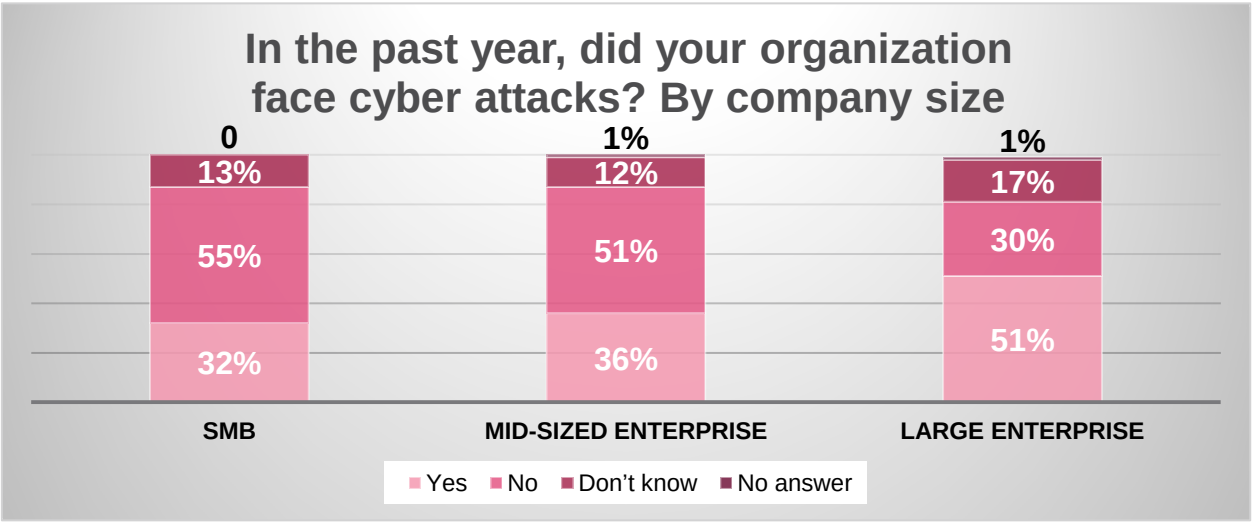
When it comes to security strategy of implementing many disparate point security products vs. a single consolidated solution, organization are almost evenly split (44-45% each).



"D DAY" – ATTACK DATA

41% of IT and Security professionals report their organization faced a cyber-security attack in the past year.

Reported attack rates are significantly higher among large enterprises of 5000 employees and above (51%).



Companies that use disparate point security solutions strategy (aka 'point solution') faced 33% more cyber-attacks.

A comparison between organizations security strategies reveals that 48% of companies that hold a disparate point products security strategy (also known as point solution) faced a cyber-attack in the past year, vs. 36% of companies that hold a security consolidation strategy.

How many? 56 cyber-attacks on average per company.

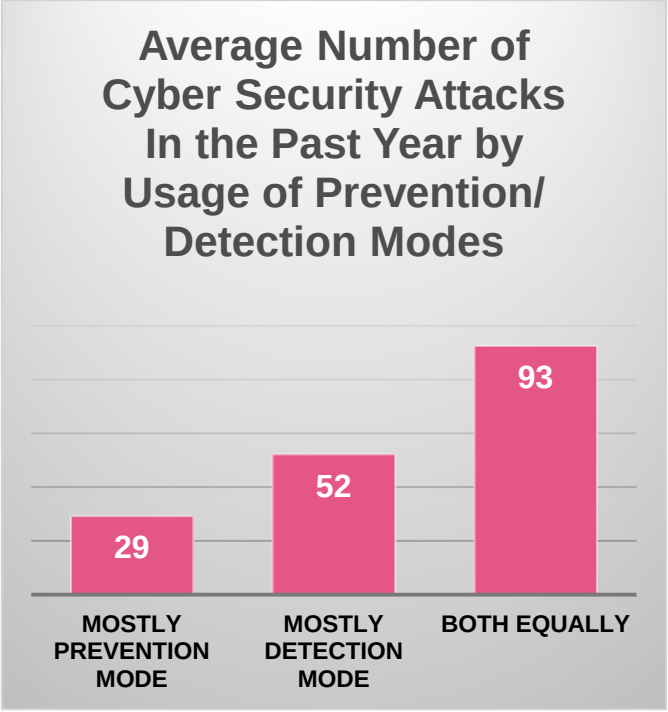
Security professionals that reported facing cyber-security attacks in the past year were asked to specify the number of attacks they faced in the past year. On average, 56 attacks were reported. Higher attack numbers were reported by large enterprises (100 attacks on average per year) and manufacturing industry companies (103 attacks on average per year).

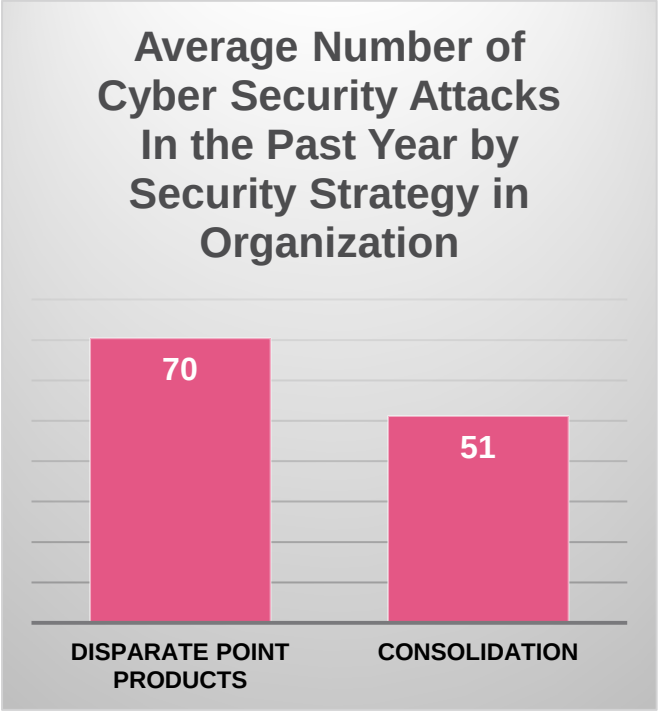
Significant differences in number of attacks by security policy

Additional survey data analysis reveals significant differences in number of attacks by cyber security approaches.

First, when examining number of cyber-attacks by prevention or detection modes used in company- companies using mostly detection mode faced 79% more attacks on average than companies implementing their security solutions in prevention mode (52 vs. 29 cyber-attacks per year in accordance).

Second, organizations that hold a disparate point security solutions policy (aka point solution) experience 37% more cyber security attacks on average than companies holding a security solutions consolidation strategy (70 vs. 51 cyber-attacks per year in accordance).





POST-ATTACK BEHAVIOR IN ORGANIZATIONS

Organizations that faced a cyber-attack in the past year report conducting a wide range of reactive activities mainly: enforcing new rules to avoid future attacks (52%), forensic analysis (52%) and/ or shut down devices suspected to be infected (49%).

Although taking various precautions, only mediocre perception of post-attack readiness (similar to pre-attack readiness).

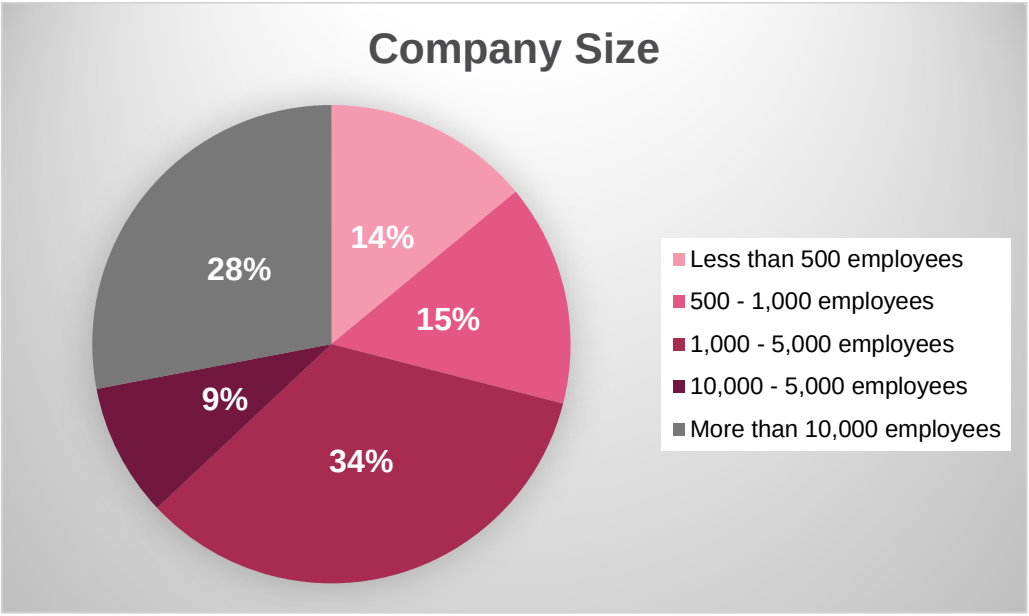
IT and Security professionals were asked to rate their overall perception of post-attack remediation readiness in their organization on a 1-5 scale (1 being very poor to 5 being excellent).

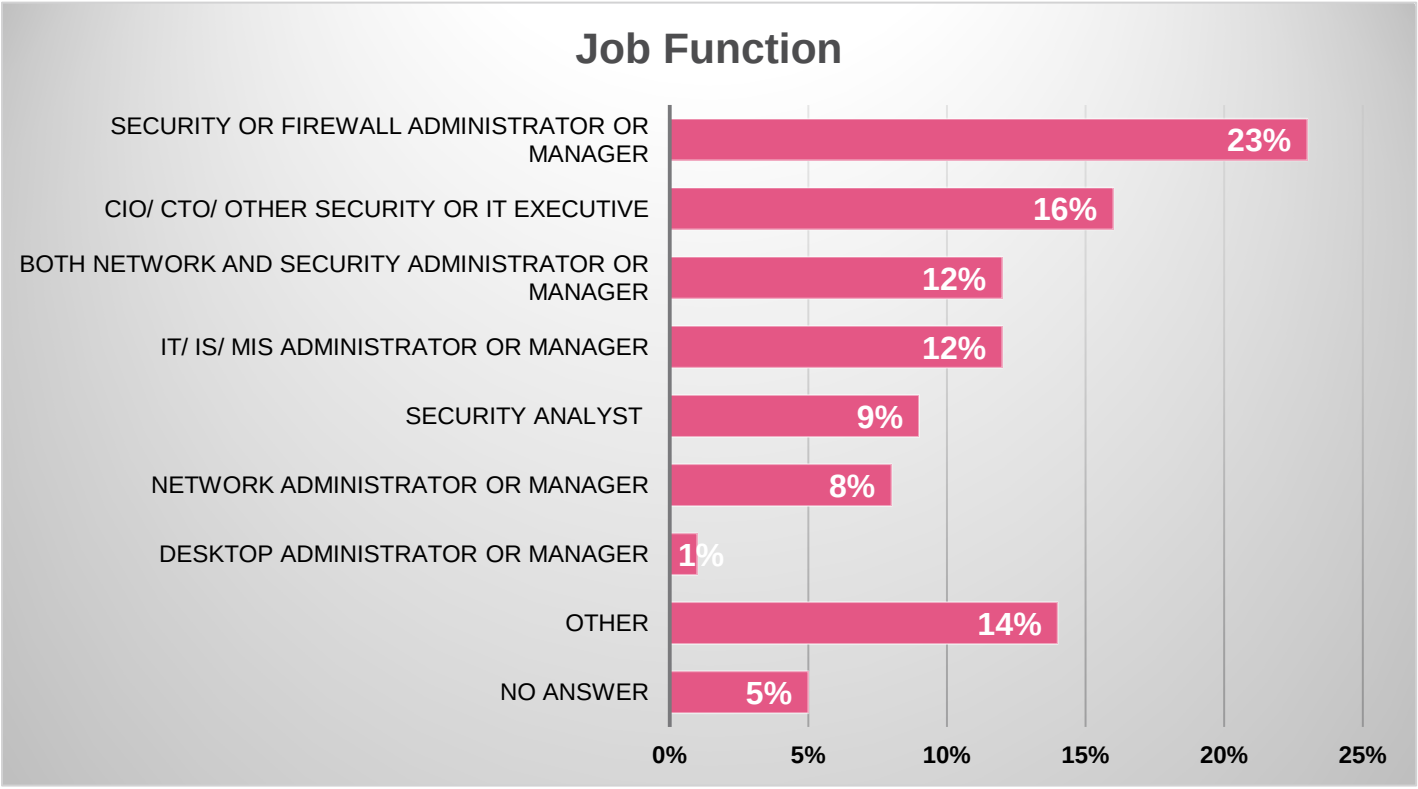
Similar to pre-attack readiness perception, Security professionals perceive their organizations to be only moderately ready in post-attack remediation circumstances, with an average rate of 3.65 on a1-5 readiness scale.

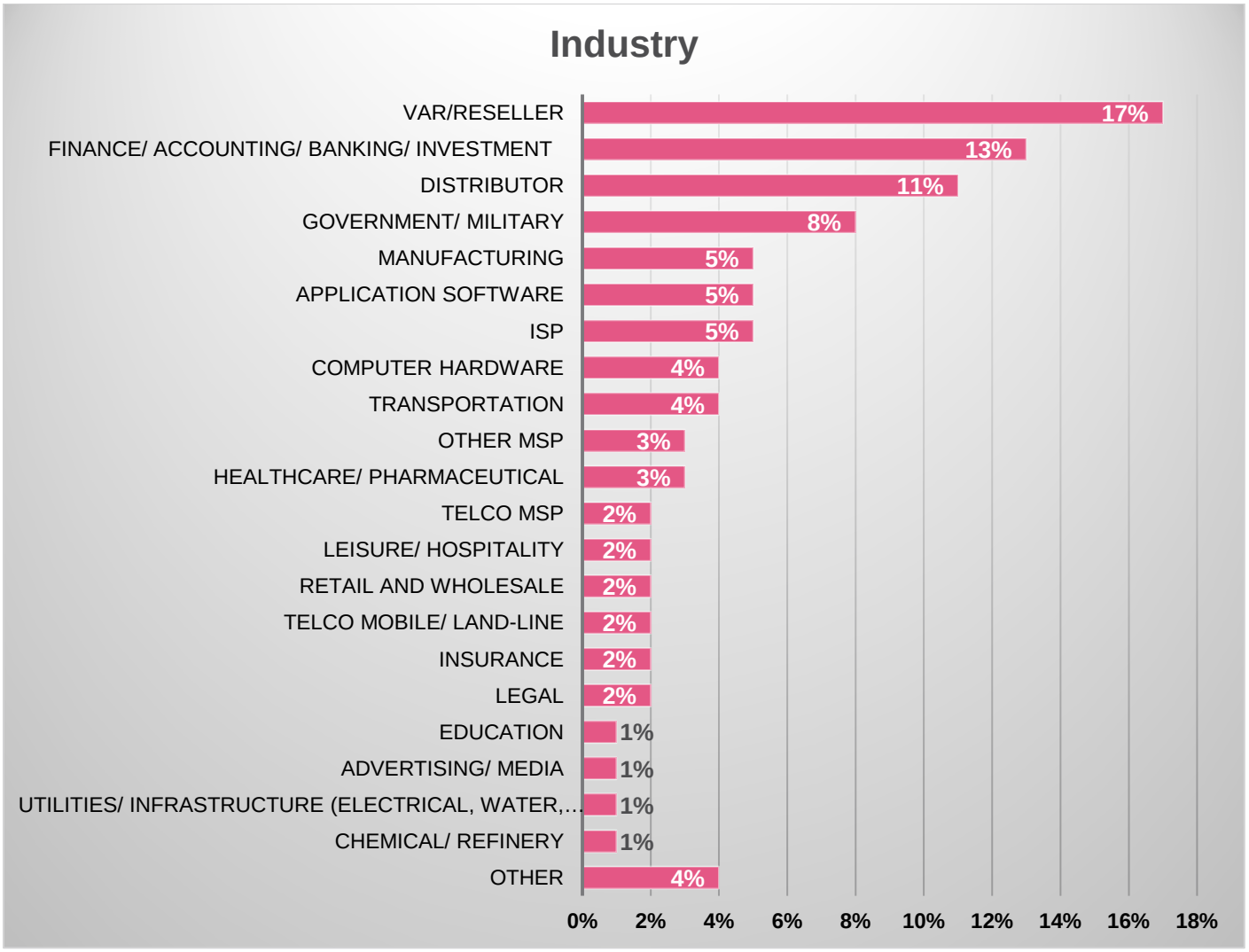
SURVEY METHODOLOGY AND PARTICIPANTS DEMOGRAPHICS

Check Point customers and Channels were invited to take part in an online survey during CPX360, Check Point's worldwide annual cyber security conference conducted in Europe, North America and Asia.

A total of 443 Security professionals answered survey. All respondents have IT security responsibility. The survey was conducted during January and February 2018.







About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Follow Check Point via:

Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

