Cybersecurity regained: preparing to face cyber attacks

20th Global Information Security Survey 2017-18

EY
Building a better working world

Findings from the Real Estate sector

The Global Information Security Survey investigates the most important cybersecurity issues facing organizations today. It captures the responses of nearly 1,200 participants around the globe from over 20 industry sectors. We base our findings and conclusions on those insights and our extensive global experience of working with clients to help them improve their cybersecurity programs.

The following findings suggest that while organizations continue to prioritize cybersecurity – and are making good progress in identifying and resolving vulnerabilities – they are more worried than ever about the breadth and complexity of the threat landscape.

Cyber resilience lost in a convergent world

In today's online world, every organization is digital by default, operating with working cultures, technologies and processes of the internet era. Moreover, in the connected and convergent world delivered by the Internet of Things (IoT), the digital landscape is vast, with every asset owned or used by the organization representing another node in the network. It has never been more difficult for organizations to map the digital environment in which they operate.

Cyber attackers roam freely in this environment. They may be either indiscriminate or highly targeted, attacking large and small organizations in both the public and private sectors. They are well camouflaged: exposing the attackers requires cybersecurity defenses that identify the threat, even when it adopts the colors of its immediate environment.

Against this backdrop, organizations must consider their resilience in the context of different categories of threat:

- **Common attacks:** These are attacks which can be carried out by unsophisticated attackers, exploiting known vulnerabilities using freely available hacking tools, with little expertise required to be successful.
- **Advanced attacks:** Advanced attacks are typically carried out by sophisticated attackers, exploiting complex and sometimes unknown ("zero-day") vulnerabilities using sophisticated tools and methodologies.
- **Emerging attacks:** These attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, typically carried out by more sophisticated attackers performing their own research to identify and exploit vulnerabilities.

Key sector findings

100% of respondents say they need up to 50% more cybersecurity budget.

80% of respondents consider a careless member of staff as the most likely source of attack.

14% feel it is very likely they would detect a sophisticated cyber attack.

76% of organizations still keep cybersecurity reporting mostly within the IT function.

58% do not have a Security Operation Center, even though they are becoming increasingly common.

17% of boards have sufficient cybersecurity knowledge for effective oversight of cyber risks.

65% do not have, or only have an informal, threat intelligence program.

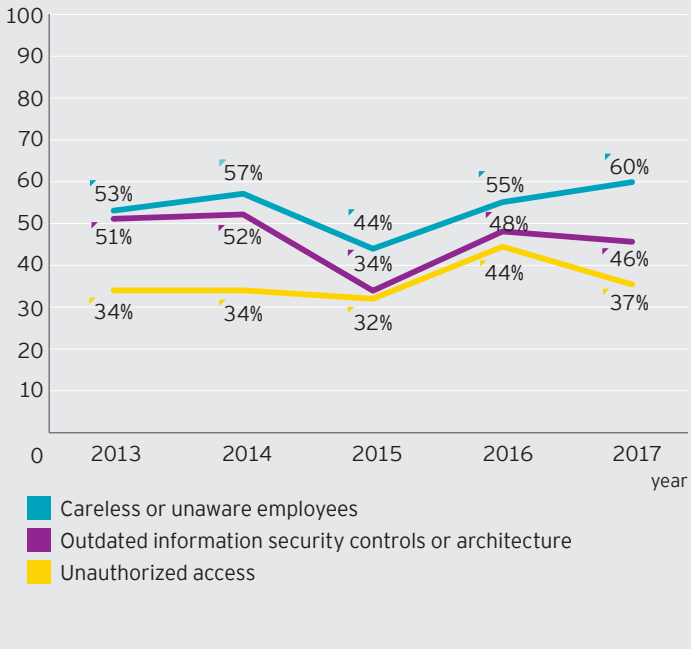
91% say their cybersecurity function does not fully meet their organization's needs.

Results (all sectors)

Threats and vulnerabilities perceived to have most increased the risk exposure of the respondents, 2013–2017

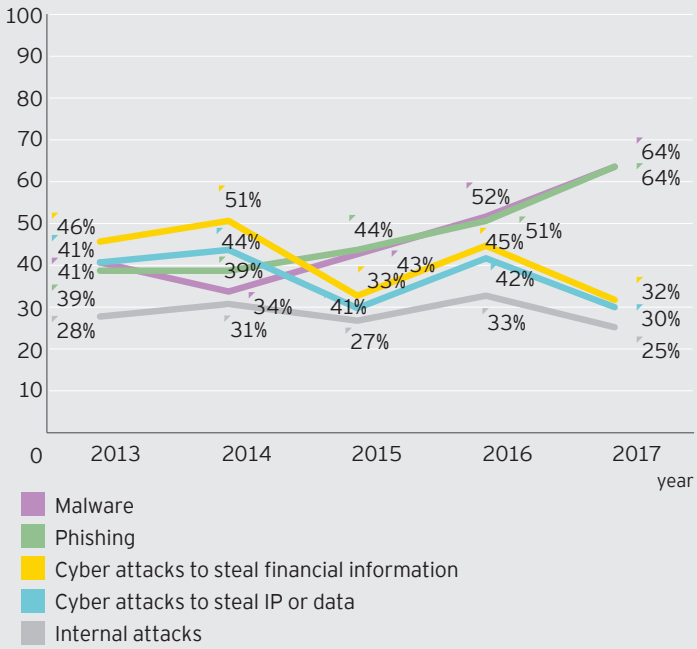
Vulnerabilities

% of respondents stating as top two items to increase risk exposure



Threats

% of respondents stating as top two items to increase risk exposure



Cybersecurity regained: building defenses that are fit for purpose ...

Organizations are likely to be confronted by a wave of attackers of varying levels of sophistication, and they can and must fight back. The response must be multilayered, with a focus on repelling the most common attacks while also introducing a more nuanced approach for dealing with advanced and emerging types of attacks. As some of these attacks will inevitably breach the organization's defenses, the focus needs to be on how quickly they are detected, and how effectively they are dealt with.

- Defending against common attack methods means closing the door to the most common types of attack. At this threat level, point solutions remain a key element of cybersecurity resilience, with tools including antivirus software, intruder detection and protection systems (IDS and IPS), consistent patch management and encryption technologies that protect the integrity of the data even if an attacker does gain access to it. Employee awareness is also a crucial frontline defense, building cybersecurity consciousness and password discipline throughout the organization.
- Defending against advanced attacks means accepting that attackers will get in and being able to identify intrusions as quickly as possible. A Security Operations Center (SOC) that sits at the heart of the organization's cyber threat detection capability is an excellent starting point, providing a centralized, structured and coordinating hub for all cybersecurity activities. SOCs are increasingly moving beyond passive cybersecurity practices into active defense – a deliberately planned and continuously executed campaign that aims to identify and remove hidden attackers and defeat likely threat scenarios targeting the organization's most critical assets.
- Defending against emerging attacks means recognizing that the nature of some threats will be unknown. Innovative organizations that are imaginative about the nature of potential future threats can build agility into their cybersecurity approach so that they are able to move fast when the time comes. Organizations with good governance processes underlying their operational approach are able to practice security-by-design – building systems and processes able to respond to unexpected risks and emerging dangers.

... developing a cyber breach response plan

Organizations are wise to operate on the basis that it will only be a matter of time before they suffer an attack that successfully breaches their defenses. Having a cyber breach response plan (CBRP) that will automatically kick in when the breach is identified represents an organization's best chance of minimizing the impact. But a CBRP must span the whole organization and it must be led by someone with the experience and knowledge to manage the organization's operational and strategic response.

For questions about cybersecurity, please contact our cybersecurity leaders:

Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
David Remnitz	+1 212 773 1311	david.remnitz@ey.com

EY | Assurance | Tax | Transactions | Advisory