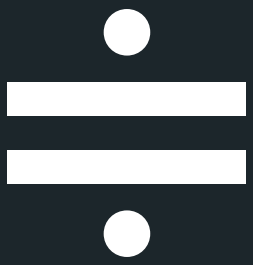
SECURITY REPORT

SURVEY REPORT SECURITY AWARENESS 2020

Solvinity
Secure Managed IT Services



Inhoud

Solvinity Security Awareness Survey Report

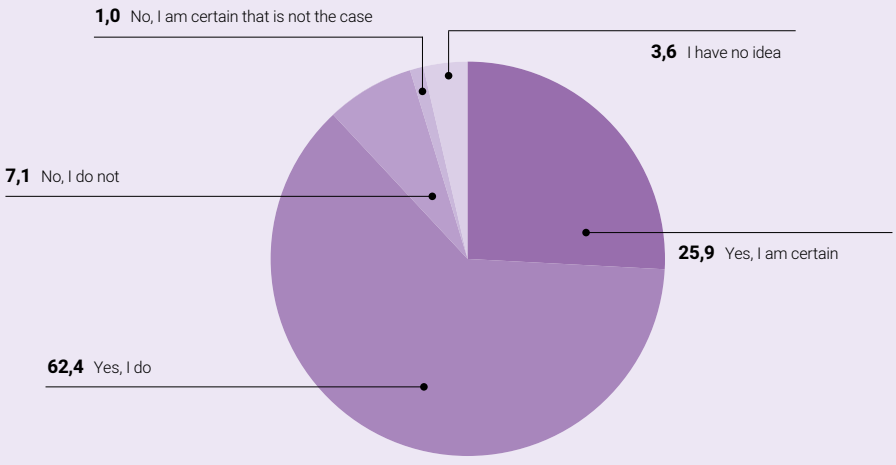
88% of Dutch IT managers say they have the security of their organisation under control, while 70% believe they are perfectly capable themselves of providing protection against cybercrime. In spite of this, 80% do not install all patches and updates and less than half take specific measures to reduce their own vulnerability. The gulf between the perception and the reality of organisations' own digital security is huge...

In July 2020, Solvinity commissioned PanelWizard to conduct a survey among more than 500 Dutch IT managers at Dutch companies with 200 or more employees, to shed light on how Dutch organisations view their own digital resilience.

The survey follows a wave of security incidents, from shutting down home servers due to unresolved vulnerabilities, to large-scale ransomware attacks and an explosive rise in cybercrime offences, which have this year exceeded the number of domestic burglaries for the first time.

In spite of these alarming developments, more than 88% of Dutch IT managers gave a positive response when asked whether their organisation has the security of the IT environment under control. 26% are certain, and 62.4% have the impression that it does. The follow-up questions in the survey clearly show that organisations often have a rose-tinted view of their own resilience.

Do you have the impression that your organisation has the security of the IT environment under control?



Lack of insight makes organisations vulnerable

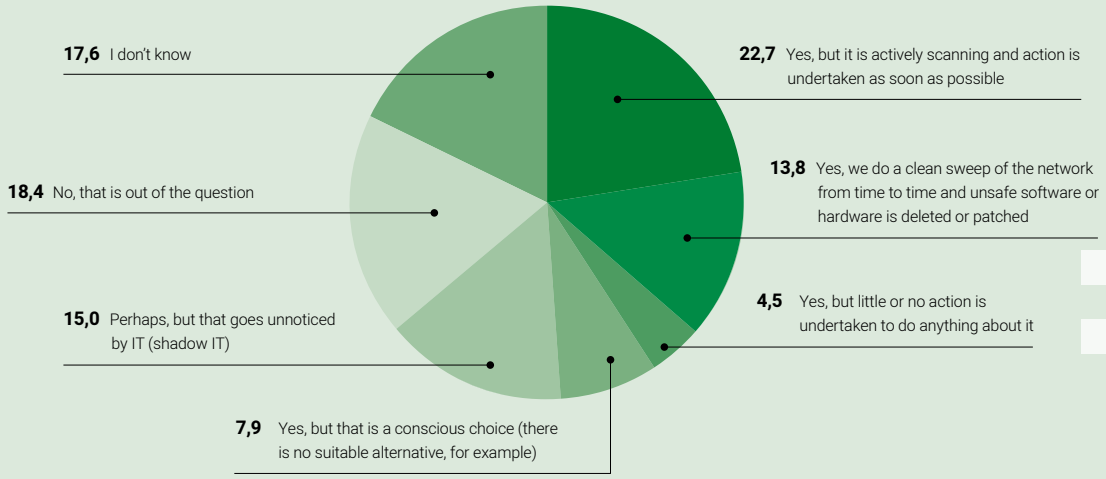
With regard to the question of whether software, hardware or services are used within the organisation which the respondents know not to be safe, 18.4% of the IT managers resolutely answered: out of the question. Marc Guardiola, CISO at Solvinity, thinks that is unlikely: "Without draconian measures, it is practically impossible to prevent devices being connected to the network, software being used or online services being clicked on from time to time, which are not approved by IT."

That is why urges that it is wise to actively scan the infrastructure, so that appropriate action can be taken immediately if such 'shadow IT' crops up in the network.

However, only 23% of the respondents do so. 14% do a clean sweep of the network periodically at best. "The remaining 63% have no idea or essentially turn a blind eye."

"Only 23% actively scan the infrastructure for undesirable hardware, software or services"

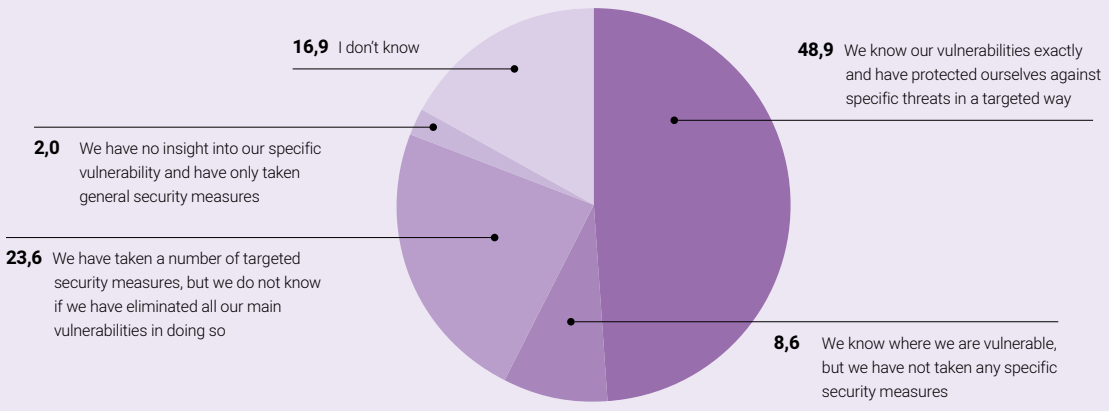
Are software, hardware or services being used within your organisation, which you know to be unsafe?



"It all begins with insight", believes Guardiola. "If you do not know where you are vulnerable, you cannot defend yourself properly." Even though every organisation should be aware of the risks they're exposed to and how they can best be covered, only 49% of respondents stated that they know precisely where their organisation is vulnerable and take targeted measures to do anything about it. The remaining 51% admitted that they are not aware of their own vulnerability or have not put any targeted measures in place. "Insight into how your IT infrastructure is organised and what goes on there is crucial to any realistic assessment of the possible risks an organisation is exposed to."

"Only 49% know precisely where their organisation is vulnerable and have put targeted measures in place"

To what extent does your organisation have insight into the vulnerability of its own IT infrastructure?



Updates and patches are sometimes not installed at all

Insight into the vulnerability of the organisation is crucial in order to take well-considered decisions about measures that are essential to the security of the organisation. One example is the approach to updates and patches. IT vendors regularly announce measures that should remedy newly-discovered vulnerabilities in their products. That also means that is generally known that they exist at that time. From then on, there is a reasonable chance that malicious parties will trying to abuse those vulnerabilities. At the beginning of 2020, a lack of clarity about the installation of patches and updates was the most important reason why a large number of Dutch companies, governmental organisations and institutions **had to take their home working solutions offline**. They did so just to be on the safe side.

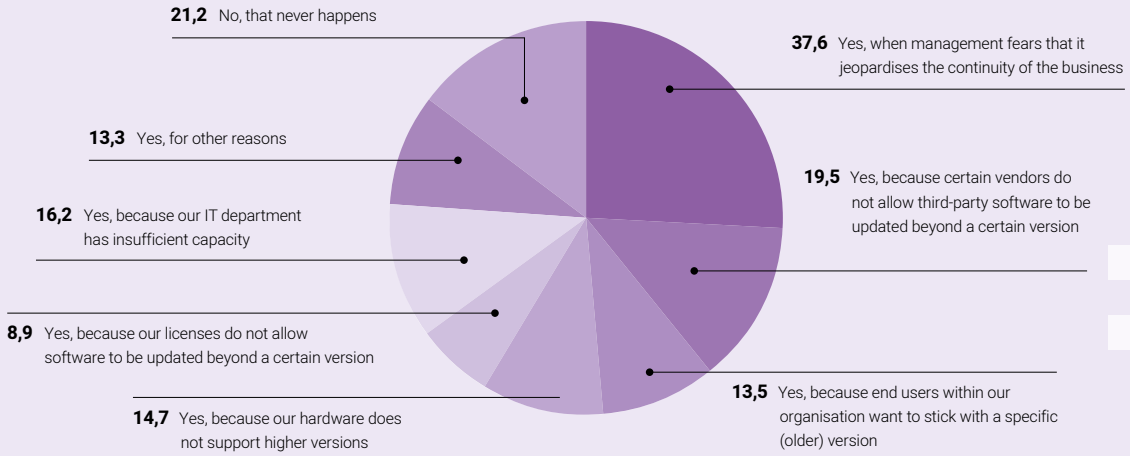
Only 49% of respondents stated that they install patches and updates that the vendor makes available within a few days. 24% need weeks to do so and 8% even wait months or longer. What's more: almost 80% stated that certain patches and updates are sometimes not installed at all. The main reason for this mentioned (38%) is that the management blocks patches and updates for fear they could jeopardise the business. "There may be legitimate reasons for that," says Guardiola. "I find it more worrying that in the case of 13% of the organisations, end users block such updates because they don't want anything to change. And even worse: 16.2% stated that the IT department has insufficient capacity to deal with patches and updates."

According to Guardiola, the risk consideration is sometimes perfectly understandable. "Installing patches and updates is not without danger. Imagine, for example, that you are running operation-critical technology, a failure of which might cost millions while the potential damage from exploitation of such a vulnerability is very small: in that case I can imagine that a company would not want to install such an update immediately, or would at least want to test it thoroughly first."

The other side to the story is that some IT used itself impedes security. 20% of respondents stated that certain vendors do not allow third-party software to be updated beyond a certain version. "Support is not longer provided if it is installed anyway", says Guardiola. A total of 14.7% stated that certain hardware is not compatible with higher software versions and 9% stated that their licences do not allow them to update certain software further. "At times like that, you are actually taken hostage by your own IT", argues Guardiola.

"Almost 80% do not install all patches and updates"

Is it (sometimes) decided within your organisation to postpone or cancel the installation of updates and patches?



NOTE: Multiple answers were possible for this question

Well-considered measures based on insight and experience

The survey also looked at the influence of IT outsourcing. Many IT departments have to contend with high workloads. In combination with the increasing complexity of IT and the rising number of security incidents, more and more organisations are deciding to outsource the management of their IT environment. The coronavirus crisis and the need to be able to guarantee business continuity even under such circumstances, appears to be reinforcing this trend. For the respondents in this survey, business continuity and the fact that IT is not one of the core tasks of the organisation are the main motivations for joining forces with a Managed Service Provider.

That is often wise from a security perspective, too, as Guardiola explains: "You simply find more people who know what they are doing at an organisation that specialises in maintaining the availability of secure IT." Solvinity clients, for instance, have less difficulty in accessing their digital work environments with ease and from any location than other organisations (66% versus 55%). However, other important differences between organisations that manage their IT themselves and organisations that (partially) outsource their IT also emerged from the study.

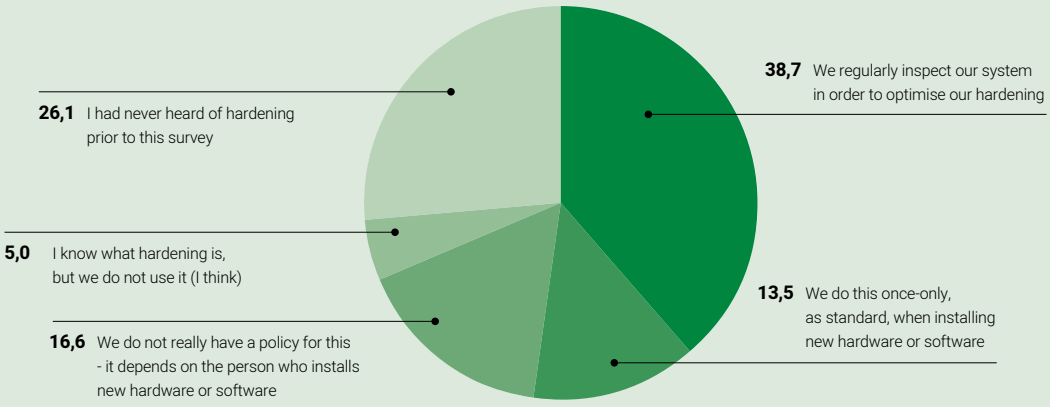
Never heard of hardening?

Respondents were asked how their organisation deals with hardening. Hardening is the process by which hardware and software settings are tested in terms of security. For instance, in order to prevent abuse, unused ports and services are closed where possible. "26% of the respondents had never heard of hardening before our survey," says Guardiola. "Mostly, these respondents did not use the services of a Managed Service Provider."

"26% have never heard of hardening"

At the same time, it was clear from the answers that not all Managed Service Providers (MSPs) are equal. "Hardening is labour-intensive", says Guardiola. "In contrast to the situation at many companies where they try to take care of security themselves, you see that most MSPs do use some form of hardening." The survey also reveals, however, that a relatively large number of service providers carry out hardening as a one-off check when installing new hardware or software. "Many outsourcers do not have a fixed policy for hardening and leave it to the specialists concerned to determine how and when they use it. That is clearly different at Solvinity," reveals Guardiola. "Continuous Hardening is standard with us: with every modification to the network, our people check that it is made as safely as possible."

Which of the statements below best describes the way in which your organisation deals with hardening?



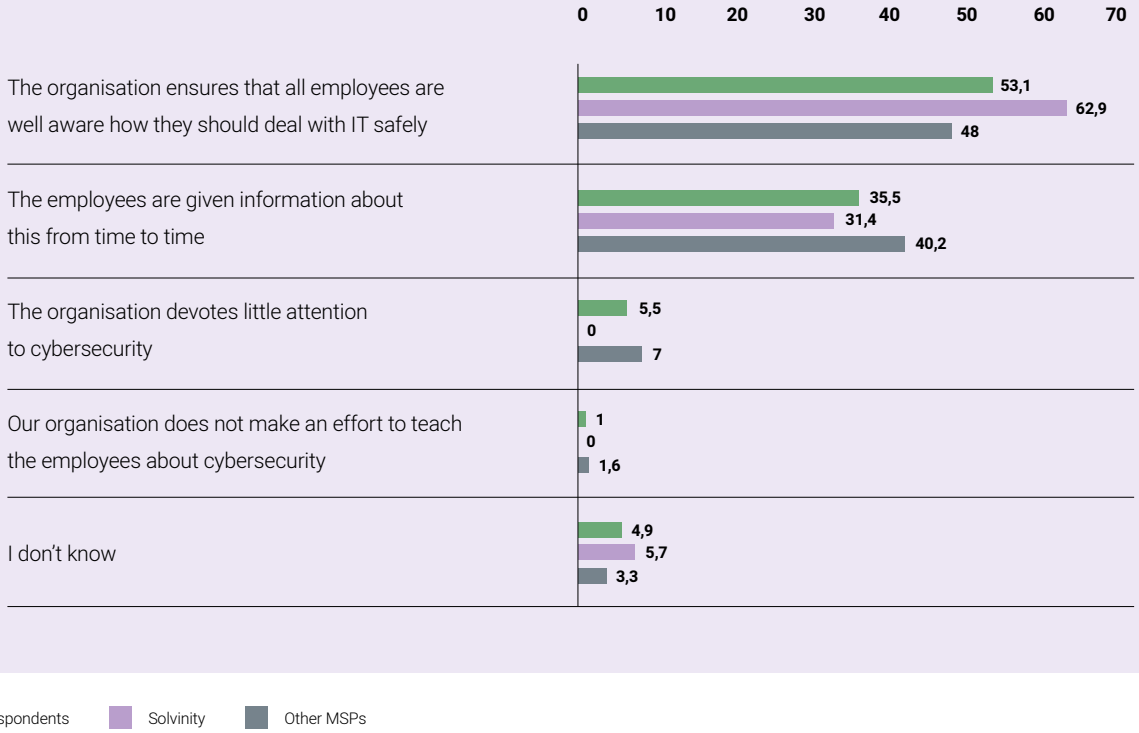
Devoting more attention to information

Another matter where differences can be seen between MSPs is the extent to which employees are informed about cybersecurity. "On average, 53.1% of respondents say that all their employees are well aware how they should deal with IT safely," says Guardiola. In the case of Solvinity clients, 63% state that everyone is properly informed, while that figure is only 48% for the other MSPs. "You therefore see that it definitely matters how much attention a Managed Service Provider devotes to cybersecurity.

Evidently, with some MSPs, the distance between business and IT has increased," notes Guardiola.

"53% ensure that all their employees know how they should deal with IT safely"

To what extent pays attention to cybersecurity among employees within your organisation?



Conclusion:

Secure Managed Services minimise risk

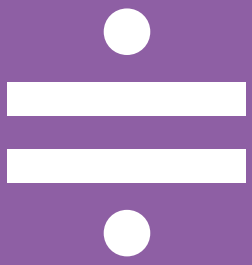
"Cybersecurity is not simple," emphasises Guardiola. "Only one thing is certain and that is that 100% security does not exist." Moreover, the tools that are available to an organisation for cybersecurity are certainly not infinite. "That means that you must continuously weigh up what the most effective measures are to minimise the risks to your specific organisation." Unfortunately, the survey shows that many organisations only have limited insight into their own vulnerability. There is therefore a considerable tendency to overestimate one's resilience.

In order to gain a realistic idea of the organisation's resilience, it is necessary to make time and resources available to gain thorough insight into the entire IT infrastructure. "Subsequently, you need people who have the knowledge and expertise to assess, together with the business, the possible risks and the most effective tools to cover those risks," says Guardiola. That does not appear to be a realistic solution for organisations in which the IT department is already under-staffed and overstretched. The best way to ensure that the organisation is protected against the most common forms of cybercrime is to rely on an experienced Secure Managed Service Provider.

About Solvinity

Solvinity provides Secure Managed IT Services in the public, private and hybrid cloud for organisations with high security requirements. Solvinity's services include innovative cloud solutions, outsourcing, managed hosting and workplace solutions such as Lango Workspace. For organisations that develop software, Solvinity offers solutions such as Integrated Delivery and "Stretched" DevOps. The organisation distinguishes itself with very high cyber security standards and certifications according to national and international standards such as ISO 27001, ISO 14001, ISO 9001, SOC 1, SOC 2 and NEN 7510. Solvinity provides services to, among others, the (national) government, including the Ministry of Justice and Security, municipalities and leading organisations in financial and business services, including Trans Link Systems (OV chip card), TNO, ING, Ahold and ONVZ. Solvinity has more than 250 employees, spread over four locations in Amsterdam, Assen, Amersfoort and Den Bosch. In 2019, the company had an annual turnover of 47.8 million euros. For more information, visit **www.solvinity.com**, or follow Solvinity on **Twitter** and **LinkedIn**.

Want to know more about Solvinity's Secure Managed IT Services?
Contact us! Call **+31 (0)20 36 43 600**
or email us at **info@solvinity.com**



Solvinity®

Secure Managed IT Services

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

T +31(0)20 364 3600
E info@solvinity.com
solvinity.com