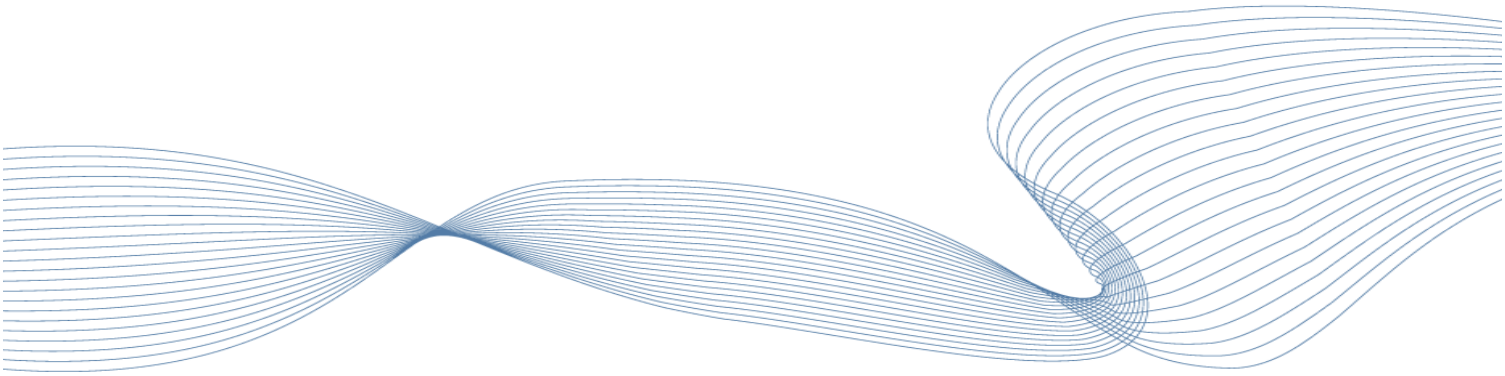
Is a cyber breach inevitable?
Cyber Security Challenges in the Netherlands

June 2015

Comissioned by:

CGI

Experience the commitment®



PAC

A CXP GROUP COMPANY

Published by

CGI

George Hintzenweg 89, 3068 AX Rotterdam, The Netherlands

Pierre Audoin Consultants (PAC) Ltd

15 Bowling Green Lane, London EC1R 0BD

Contact:

Duncan Brown (+44 [0]20 7553 3966 d.brown@pac-online.com)

CONTENTS

1. Introduction 4
2. From breach prevention to breach detection 5
3. Why Breaches Are Inevitable 7
4. How The Netherlands compares with other countries 9
5. The Business Impact of Cyber Breaches 11
6. Sector and company size differences 12
7. Conclusion 14
8. Methodology 15

1. INTRODUCTION

Many organizations have the experience of being attacked by cyber criminals, and the threat continues to grow. But are defences adequate to keep attackers at bay?

This white paper argues that cyber security breaches are inevitable, due to three compelling forces that sit outside the control of most organizations. It examines whether organizations in the Netherlands are prepared for the inevitability of cyber breaches, and illustrates the shift in spend from Prevent & Protect activities to those focused on Detect and Respond.

There are some interesting comparisons to be made between the Netherlands and other neighbouring countries that are discussed in the paper, and we also look across different sectors and company sizes to draw some conclusions about what Dutch firms should do in an age of the inevitable breach.

2. FROM BREACH PREVENTION TO BREACH DETECTION

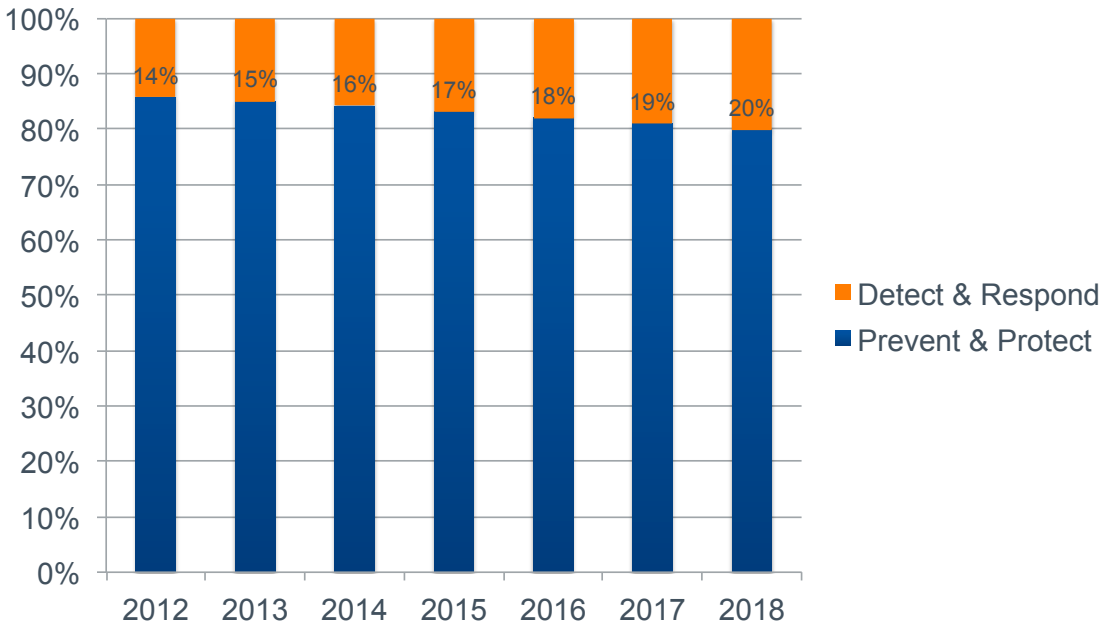
How do firms cope with the inevitable breach? We're seeing a shift in spending from breach prevention to breach detection and remediation. It indicates that organizations understand that many of the sources of threat are beyond their control.

The traditional approach to cyber security has been to build a wall around the enterprise's IT infrastructure perimeter to keep out malicious threats. As the threats increase and diversify the wall keeps getting higher. But attackers are creative types, and they have developed new methods to circumvent such preventative measures. They tunnel under the walls, or find an unguarded door or window, or persuade the gatekeeper to lower the drawbridge. Once the attacker is in, what then?

This perimeter-based approach is necessary but not sufficient. We need high walls. But we must also plan for what happens when the walls are breached, or subverted.

> *"Traditionally, firms have spent around 85% of their cyber security budget on Prevention technologies, and only 15% on Detect and Respond. As breaches become inevitable, this ratio has to change."*

Traditionally, firms have spent around 85% of their cyber security budget on Prevention technologies, and only 15% on Detect and Respond (see chart). As breaches become inevitable, this ratio has to change. As organisations realise that breaches are inevitable they are shifting cyber security spend away from protecting the perimeter to planning to detect and respond to a breach. In fact, the rate of growth of spend on Detect and Respond is 14%pa, twice the overall market growth rate.



Share of Netherlands cyber security spend, 2012-2018 (forecast). Source: PAC

Importantly, although overall cyber security budgets are also rising, at 7.3% CAGR to 20118, they are increasing much more slowly than Detect & Respond activities. So spend on Detect & Respond will inevitably divert spending away from Prevent & Protect activities.

However, although the spend on Detect & Respond is increasing it is insufficient. Once an attacker has penetrated defences they can wreak havoc inside an organization. If over 80% of budget is being spent on Prevent & Protect it leaves less than 20% on discovering and dealing with breaches. Given the potential severity of breaches, speed of discovery is critical.

PAC thinks that organizations should be aiming at spending one third of their cyber security budget on Detect & Respond, at least until technology and skills catch up and provide comprehensive coverage.

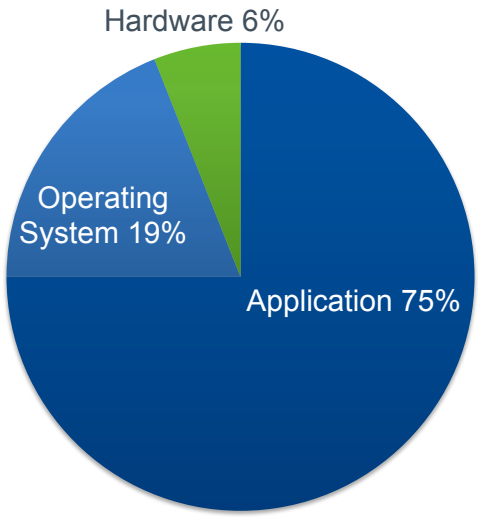
3. WHY BREACHES ARE INEVITABLE

Organisations in the Netherlands are under attack from a variety of cyber threat actors. All of the current metrics that measure the rate of threat increase, the extent of breaches and the business impact suggest that the chances of a breach occurring in any organisation is highly likely, and may be inevitable:

- The number of incident reports that the NCSC handled during 13/14 is "considerably higher than the number" in the previous year, showing a year-on-year increase of over 200%[1].
- The number of reported incidents rose in the private sector, from 37% to 46% of all reports[2].
- Breach detection rates are poor. The average time to discover a breach within an organisations is 229 days[3].
- Insurance companies that write cyber risk insurance policies do so on the basis that a claim is 100% likely[4].

There are three reasons why cyber security breaches are inevitable. Importantly, these reasons sit outside the control of most organizations, in that they are environmental or market failures.

1. The shocking state of application development today.



The vast majority of vulnerabilities, 75% in total, in today's IT systems are found in applications[5]. Mostly these are commercially produced applications, commonly browsers but also popular web-based apps and

[1] Source: NCSC Cyber Security Assessment Netherlands CSAN-4, October 2014
[2] ibid
[3] Source: Mandiant
[4] Source: Beazley
[5] Source: US National Vulnerability Database, PAC estimates

– increasingly – mobile apps. Such is the rate of app proliferation that testing and version control seems a distant memory. This 'appification' of software has led to the deprofessionalisation of app development.

The reality for organizations today is that they must assume commercial apps are major sources of vulnerabilities.

> *"The vulnerability of software and systems remains relentlessly high. This does not seem to change. … At present there is no solution for this issue."*
>
> National Cyber Security Centre
> Cyber Security Assessment Netherlands CSAN-4

2. The malicious insider threat

Few organizations have the processes and systems in place to detect behavior from employees and contractors that expose them to cyber threats. Many staff have intimate knowledge of a system, or know those that do, and can subvert security processes and checks to steal information. Most security systems check for unauthorized intrusion, but the most dangerous threat comes from the authorized - but malintended – user. Fourteen percent of all breaches are caused by internal actors[6].

Privileged access management (PAM) tools are the latest means of trying to detect such behavior. Behavioral analytics is also an increasingly common approach. But such mechanisms are still rare. Edward Snowden is the archetypal modern insider, but the history of insiders is as long as the history of espionage. Again, the reality for organizations is that they must assume an insider threat.

3. The hapless user.

"There's no patch for stupidity," says Kevin Mitnick[7]. While one may agree with the veracity of this statement the sentiment is incorrect. Many security professionals berate users for doing "stupid" things. Like writing their passwords down, or using easy-to-guess passwords, or clicking on authentic-looking email links, or losing their laptops on trains, or sending unencrypted emails containing sensitive information, and so on.

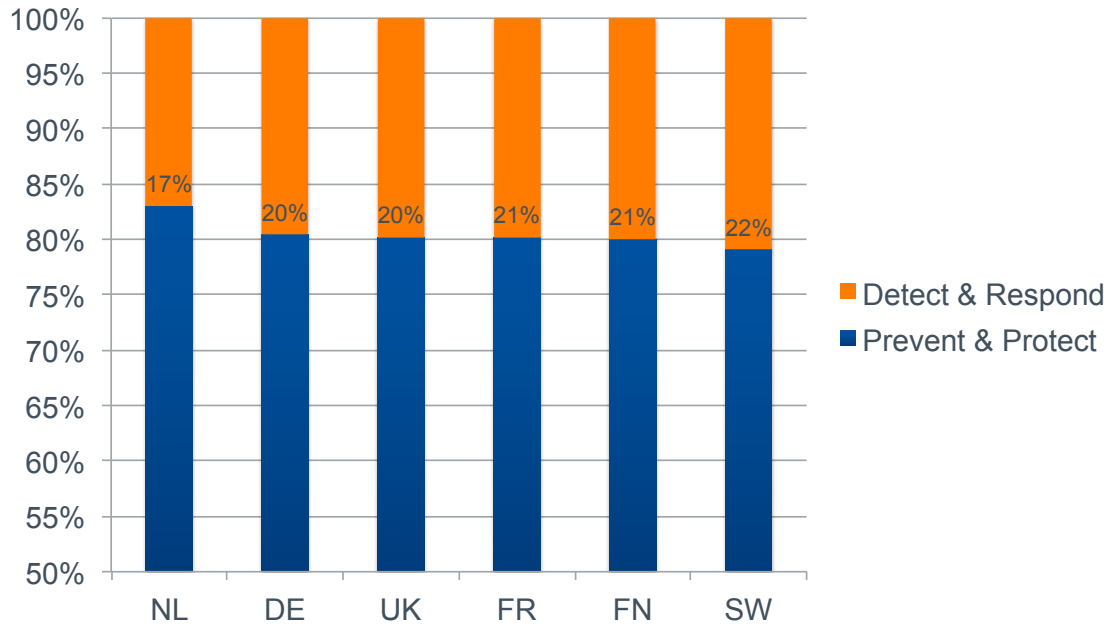
The truth is that users find navigating IT systems difficult. The IT industry has made systems too hard for the majority. Until organisations make security easy for users, preferably invisible and embedded within systems, and eliminate passwords, they must assume that users will be a weak point in defence.

[6] Source: Verizon Data Breach Investigation Report 2015
[7] Kevin Mitnick, computer security consultant, author and hacker. Formerly the most-wanted computer criminal in the United States

4. HOW THE NETHERLANDS COMPARES WITH OTHER COUNTRIES

4.1 The Netherlands lags EU competitors in spend on Detect & Respond

When it comes to spend on Detect & Respond products and services, the Netherlands lags its main competitors in the EU. In 2015 PAC estimates that only 17% of cyber security spend will be directed towards Detect & Respond (see chart). In contrast, Germany and the UK spend 20%, France and Finland 21% and Sweden 22%.



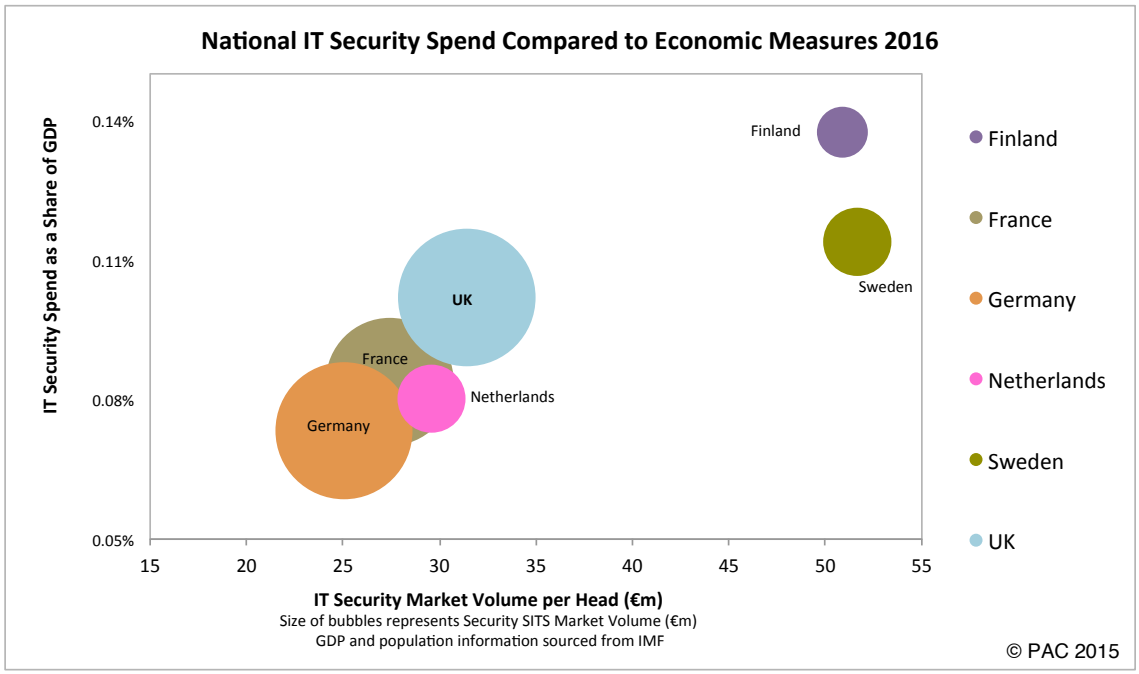
Share of cyber security spend 2015 (forecast), selected countries. Source: PAC

This means that Dutch firms are behind the curve on preparedness for cyber attacks, compared with their European neighbours. This doesn't impact firms' vulnerability to attacks. But it does impact their ability to detect attacks early, their ability to respond and remediate attacks, and it may increase the impact of an attack on business.

4.2 Overall spend on cyber security is lower than for comparsble markets

Compared to other countries in the EU, the Netherlands spends a similar amount on cyber security than its larger neighbours in France, Germany and the UK, as a proportion of GDP. It also spends around the same as a proportion per head of population. But is is much lower on both counts than Finland and Sweden. This is important as these countries have an IT Security market comparable to that in the Netherlands.

The conclusion is that the Netherlands is spending proportionately as much on security as a large country, but without the economies of scale that large countries benefit from.

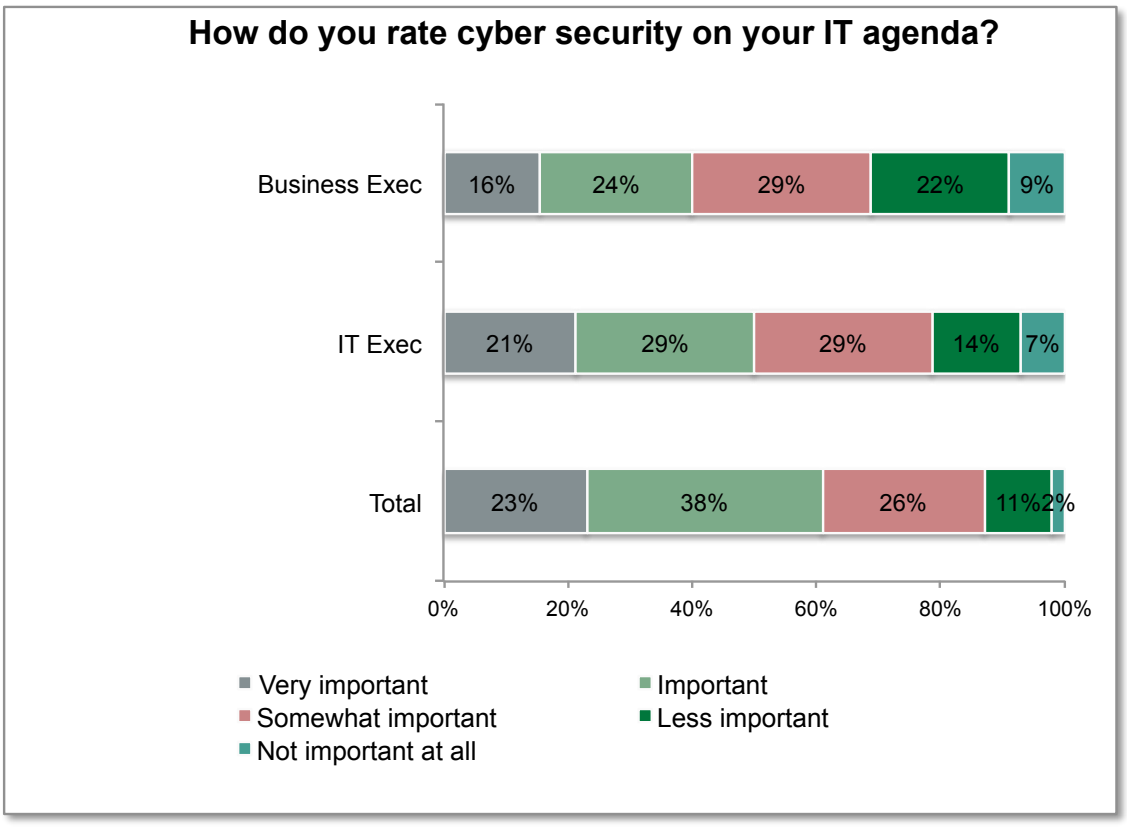


This may indicate that Dutch enterprises are underspending on cyber security, and may therefore see it as less of a priority than its Nordic neighbours. The Netherlands could spend an additional 0.03% of GDP on cyber security to close this funding gap.

5. THE BUSINESS IMPACT OF CYBER BREACHES

There is no doubt that cyber breaches are now a business issue. The impact of a serious breach can have substantial effect on financial performance and reputation, affecting future performance and share price. It's not surprising, therefore, that business and IT executives share broadly the same views when it comes to the general importance of cyber security (see chart below). There are slight differences in their regard to the importance of cyber security generally, but nothing significant that will worry security budget holders.

However, there are core differences between IT and business approaches to remediating a breach, with IT managers preferring a more technical solution through automated security. Business executives are more willing to adopt outsourcing of Incident Response as a means of alleviating the increased workload[8]. Interestingly, business people are much less willing to adopt cloud-based security functionality. The cloud is often still seen, incorrectly, as an insecure platform[9].

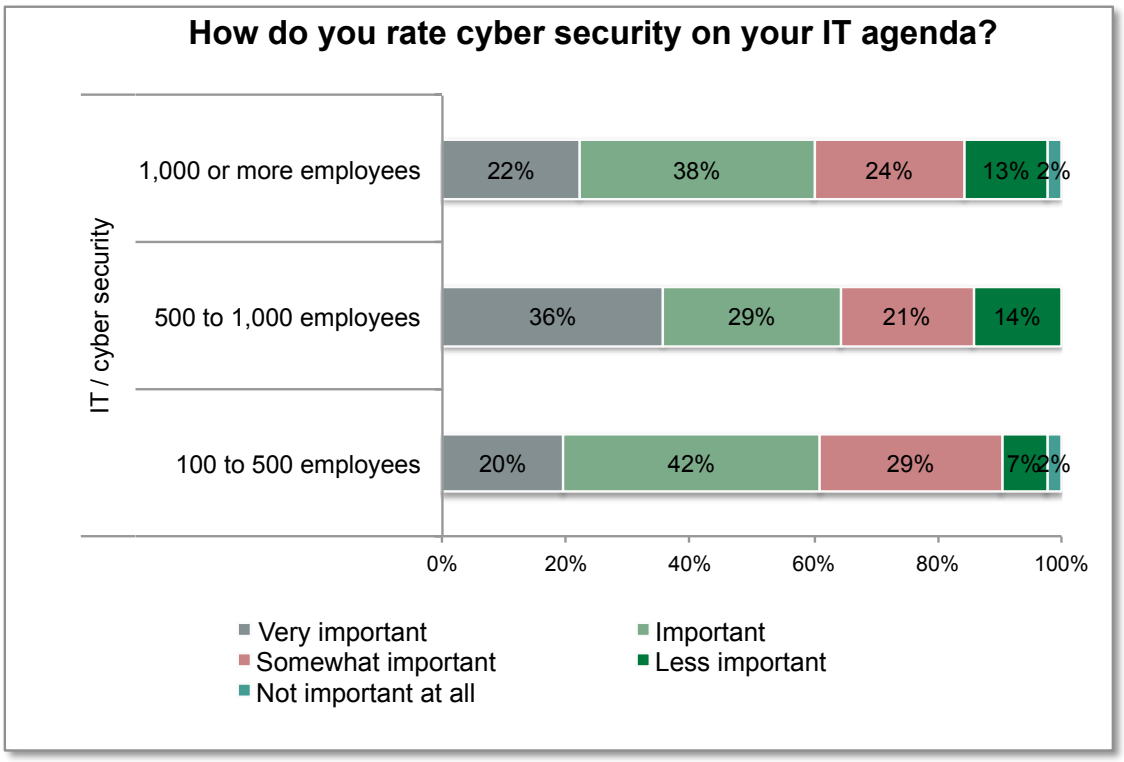


Share in percentage of all companies in the Netherlands, n = 100

[8] Source: PAC, Is cyber security now too hard for enterprises? 2015
[9] Source: PAC: Securing the Cloud, 2014

6. SECTOR AND COMPANY SIZE DIFFERENCES

There are some interesting differences between firms of varying sizes in the Netherlands when regarding attitudes to cyber security (see chart). Broadly, the smaller the firm the more important cyber security is to it. This is because of the swathe of media stories highlighting the increasing cyber threat, and because smaller firms are generally less well prepared to cope with a cyber incident. In fact, many smaller organisations knowlingly accept cyber risks in favour of prioritising buisness agility[10]. They are also averse to spending on technology that may not provide gains in productivity or competitive advantage. Importance of a topic does not necessarily translate into budget made available.



Share in percentage of all companies in the Netherlands, n = 100

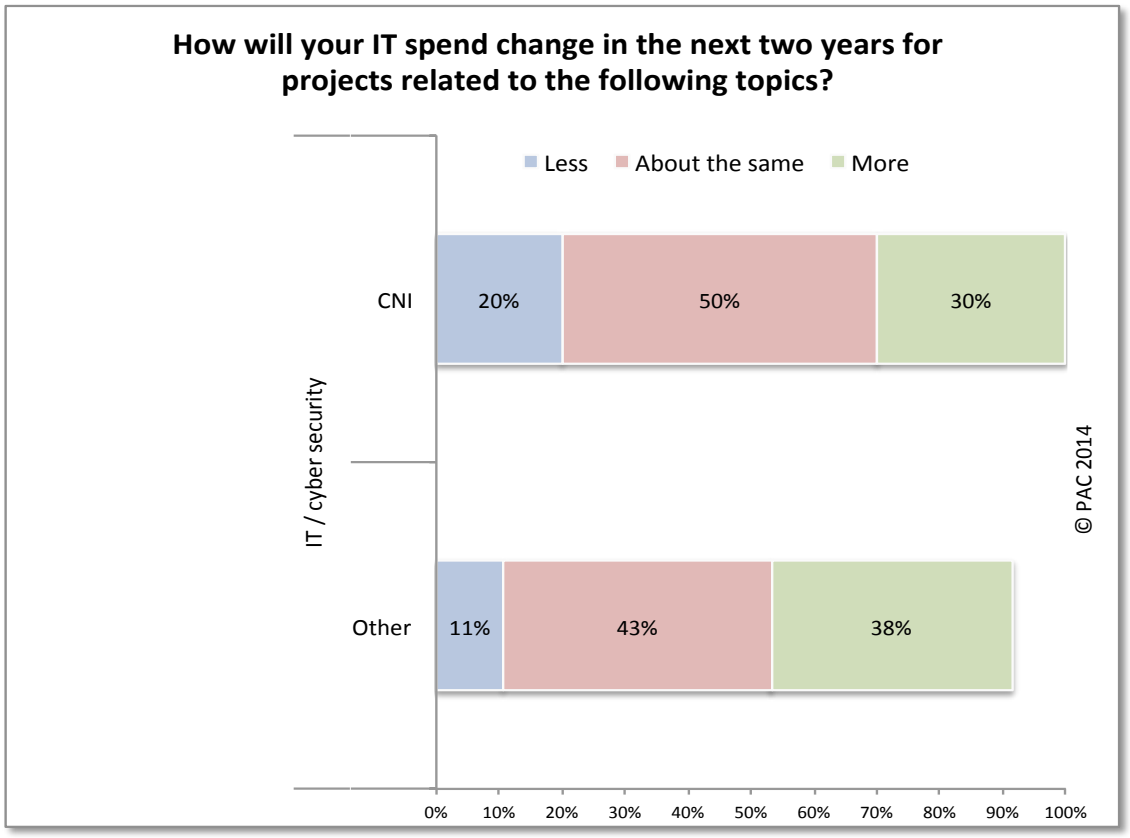
Larger organisations generally have a more mature and balanced approach to cyber security, because the business risks and potential impact are greater. They have in-house staff with cyber security expertise on which to draw, though these staff are under increasing pressures. A recent PwC report noted that, "when it comes to discovering incidents, one thing is very clear: large companies have the edge over small companies."[11] "Larger companies typically have more mature security processes and technologies in place, which allows them to uncover more incidents," it explains.

[10] Source: The Economist Intelligence Unit
[11] Source: PwC, Global Information Security Survey 2015

In terms of sector differences, industries involved in critical national infrastructure (CNI), such as Transport, Energy, Financial Services, and Telecommunications, generally are better prepared for cyber security incidents. Defence is a special case, as it is publicly funded: other public sector divisions are relatively weaker at cyber security, especially Local Government and Education. Retail, Media and Professional Services also struggle with cyber security and are less mature.

This situation is because of the extent of attacks on CNI firms. Transportation, communications, electric, gas & sanitary services were the most targeted organisations in the Netherlands, accounting for 36% of targeted attacks, according to Symantec. Financial Services are a close second, with almost 26% of targeted attacks[12]. The more an organisation is attacked the more it focuses on Detection and Response.

However, there is some difference in cyber security spending patterns between CNI and non-CNI organisations in terms of intent to increase budgets. Thirty percent of Dutch CNI firms intend to increase cyber security spending in the next two years, whereas 38% of Dutch non-CNI firms will spend more on cyber security. So the gap in maturity – and Detection and Response – may be closing: as organisations mature they tend to spend more of their cyber security budgets on Detection and Response.



Share in percentage of all the companies in the Netherlands that rate the topic at least as somewhat important, n = 87

[12] Symantec Internet Security Threat Report 2014: The Netherlands: Internet Security Threat Profile

7. CONCLUSION

The cyber security threat is growing, and shows no signs of slowing down. Organizations are under pressure to vigorously defend themselves, but the number and growth of application vulnerabilities, together with the ineradicable twin issues of malicious insiders and hapless users, means that breaches will occur.

So what should Dutch firms do? First, we are already seeing a shift in spend away from Prevent & Protect activities – and mindset – towards Detect & Respond. This must continue, and quicken. Dutch firms are behind the curve compared to their EU neighbours and need to catch up, in terms of overall spend on cyber security, and in shifting spend to breach response. The Netherlands is an attractive target for cyber attackers, yet its readiness appears to be below that of comparable countries.

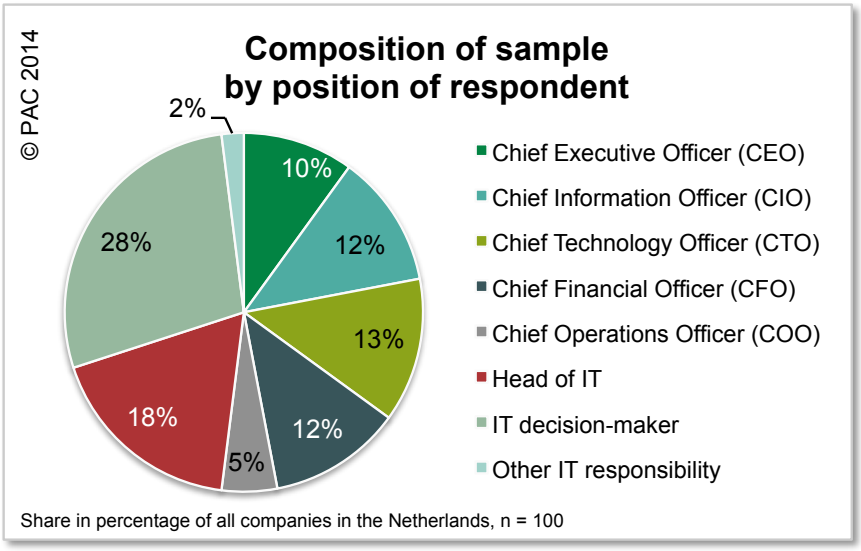
PAC thinks that few organizations, in the Netherlands or any other country, are spending enough on Detect & Respond. Even the more advanced countries spend less than one quarter of their cyber security budgets on this area. Discovering breaches is hard, as the average time for breach detection shows. Organizations need to get better at this important skill and, at least in the short term, should draw on the expertise and experience of cyber security specialist providers.

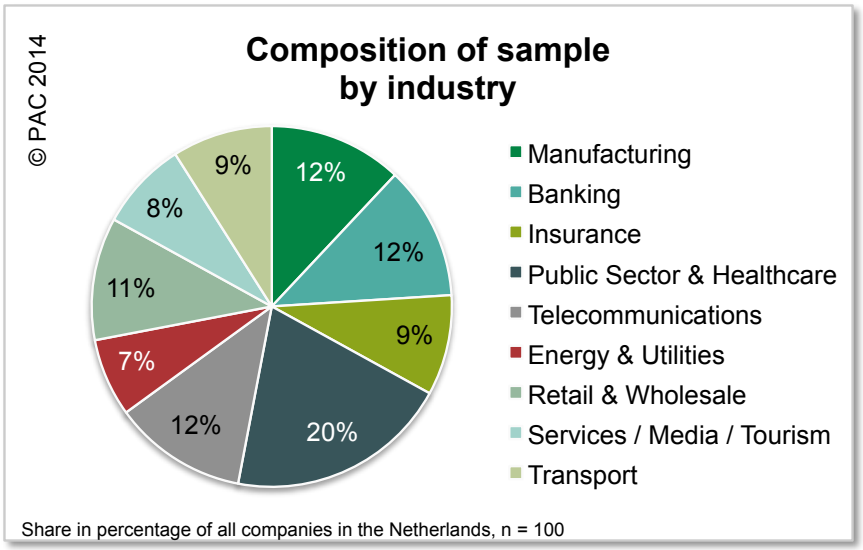
8. METHODOLOGY

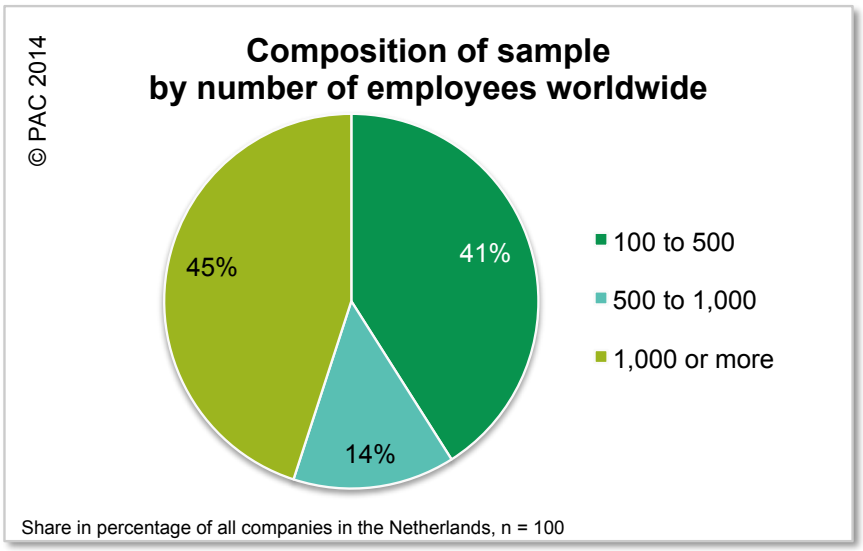
8.1 Survey

PAC conducts an annual "SITSI® CXO Investment Survey," interviewing around 1,800 decision makers in user companies all over the world to get their views on current IT trends, key requirements and investment plans.

The survey results used in this document are drawn from the CXO Investment Survey, conducted between September and November 2014, and uses responses from firms in Netherlands. The survey sample comprises companies with more than 100 employees, from all industries. In the Netherlands, 100 companies participated in the survey. The interviews were conducted with IT decision makers and other executives with IT responsibility (see graphs below).







8.2 Forecasts

The forecasts provided in the document are from PAC's Market Figures - Security by Segments, Netherlands, 2012 to 2018, published in October 2014.

ABOUT CGI

Founded in 1976, CGI Group Inc. is the fifth largest independent information technology and business process services firm in the world. Approximately 68,000 professionals serve thousands of global clients from offices and delivery centres across the Americas, Europe and Asia Pacific, leveraging a comprehensive portfolio of services including high-end business and IT consulting, systems integration, application development and maintenance, infrastructure management as well as a wide range of proprietary solutions.

Cyber security is part of everything we do and for over 35 years, our government and commercial clients have regarded us as their cyber security expert of choice. Cyber-attacks are becoming more sophisticated and can cause financial loss, reputational damage, theft of business critical information or regulatory fines. We have helped our clients build cyber security into their corporate strategy so they can conduct business in a digital age with confidence, openly and globally, driving competitive advantage, efficiency and growth.

Find our more at cgi-group.co.uk/cybersecurity or contact us on cybersecurity@cgi.com

ABOUT PAC

Founded in 1976, Pierre Audoin Consultants (PAC) is part of the CXP Group, the leading independent European research and consulting firm for the software, IT services and digital transformation industry.

The CXP Group offers its customers comprehensive support services for the evaluation, selection and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, the CXP Group supports ICT decision makers in their digital transformation journey.

Further, the CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organizations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, the CXP Group provides its expertise every year to more than 1,500 ICT decision makers and the operational divisions of large enterprises as well as mid-market companies and their providers. The CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center) and Pierre Audoin Consultants (PAC).

For more information please visit: www.pac-online.com