

REPORT

proofpoint®

**PEOPLE-CENTRIC CYBERSECURITY:
A STUDY OF IT SECURITY
LEADERS IN THE NETHERLANDS**

EXECUTIVE SUMMARY

The cyber threat landscape in the Netherlands is rapidly evolving, with cybercriminals increasingly targeting people rather than infrastructure.

From email-based threats, such as Business Email Compromise (BEC), to credential phishing, compromised cloud accounts and debilitating ransomware attacks, cybercriminals are aware that employees can easily be tricked. Using social engineering techniques, cybercriminals steal credentials, siphon sensitive data, and fraudulently transfer funds. Employees across all job levels and functions can put your business at risk in numerous ways, from using weak passwords and sharing credentials to clicking on malicious links and downloading unauthorised applications.

To address this, organisations must consider how often they are being targeted, the risks these attacks pose and how prepared they – and more importantly, their workforce – are. Employee education and security awareness is often the difference between an attempted cyber attack and a successful one.

To better understand how people-centric cyber attacks are impacting organisations, Proofpoint commissioned a survey of 150 CSOs/CISOs across the Netherlands. The study, conducted by research firm Censuswide, surveyed organisations with 200 or more employees, with a natural fallout across industries in April 2020.

The study explored three key areas:

- Frequency of cyber attacks
- Employee and organisational preparedness
- Challenges to implementing cyber strategies

The study found that the need to protect people from imminent threats has never been greater, with the majority of organisations in the Netherlands experiencing at least one cyber attack in the past 12 months. From board level buy-in, to upping cybersecurity awareness training, organisations need to take steps to shore up their cyber defences.

This report highlights these and other key insights from the survey.

FINDING 1: ORGANISATIONS IN THE NETHERLANDS ARE FACING A DIVERSE THREAT LANDSCAPE

There is no doubt that organisations globally are facing a fast-evolving threat landscape, and the Netherlands is no exception.

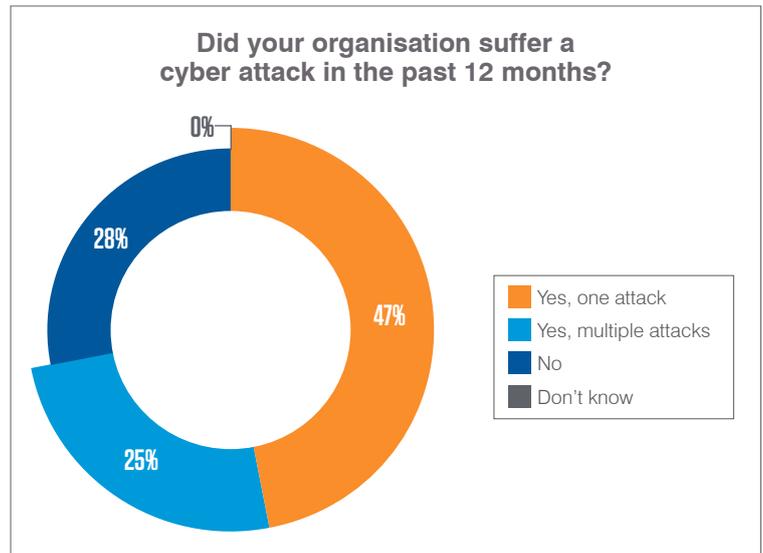
Our survey revealed that 72% of CSOs/CISOs said their company suffered at least one cyber attack in the past 12 months*. 25% said that their business was targeted multiple times.

Insider threats on the rise and cybercriminals zone in on credentials

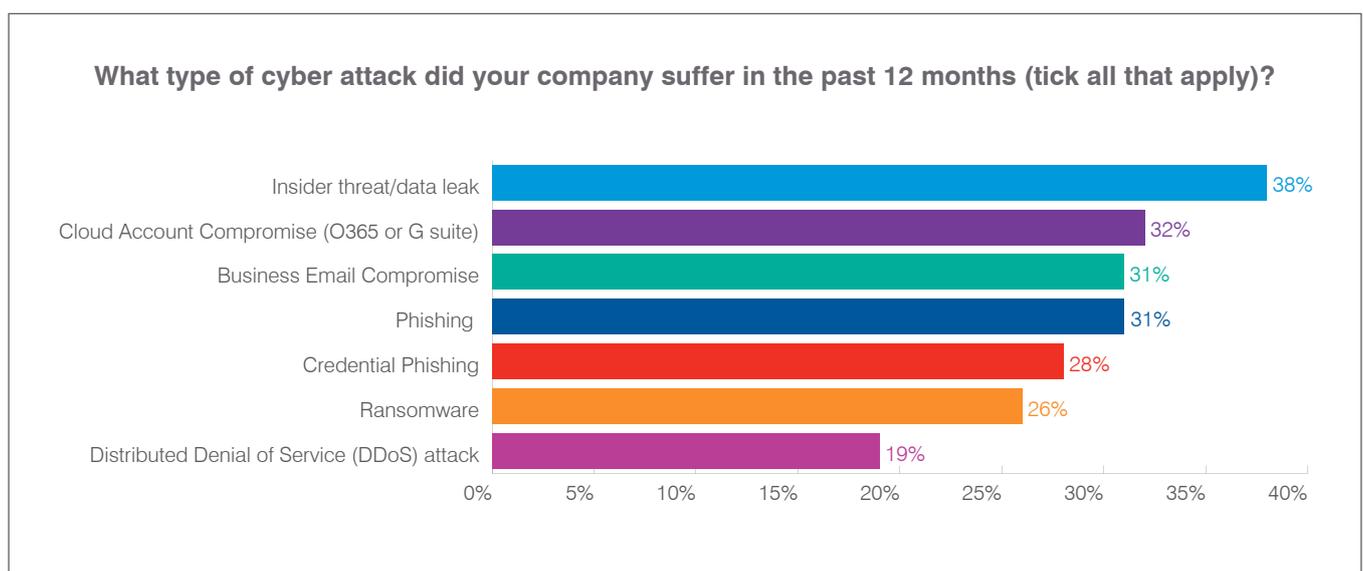
The 2020 Ponemon Institute [Cost of Insider Threats report](#) shows that insider threats are a growing concern for businesses, with the number of incidents up by a [staggering 47 percent in just two years](#). This is reflected in this survey, with 38% of Dutch CSOs/CISOs saying their businesses were victims of insider threats in the past year.

Meanwhile, cybercriminals are increasingly using compromised credentials to access email accounts, sensitive information and corporate systems. Credentials are often phished via email – a method of attack that remains alarmingly effective.

Our research found that cloud account compromise was the second leading method of cyber attack in the Netherlands in the past 12 months, impacting 32% of companies, followed by Business Email Compromise (31%) and phishing (31%).



72% of organisations in the Netherlands suffered at least one cyber attack in the past 12 months.



*Combining 'Yes, one attack' and 'Yes, multiple attacks'

FINDING 2: CSOS AND CISOS IN THE NETHERLANDS MOST CONCERNED ABOUT DECREASED CUSTOMER BASE AND FINANCIAL LOSS DUE TO CYBER ATTACKS

Cyber attacks of any nature can have devastating consequences for the organisations involved.

The World Economic Forum estimates that between 2019 and 2023, [\\$5.2tr in global value will be at risk](#) from malicious actors. From lost revenues and reputational damage to downtime, legal fees, compensation and remediation, the financial impact of such attacks can be far-reaching.

Email fraud via Business Email Compromise (BEC), in which an attacker gains access to an email account and spoofs its owner, is also on the rise – and can prove costly. The latest FBI report [estimates total worldwide losses as a result of BEC at \\$1.7bn](#) in 2019.

Our survey revealed that nearly half (49%) of businesses in the Netherlands cited decreased customer base as the biggest consequence of a cyber attack – followed by financial loss (41%) and business and operational disruption (39%). Brand/Reputation damage (38%) and data breaches (36%) are among the other common consequences cited.

49% of businesses in the Netherlands cited a decrease in customer base as the biggest consequence of a cyber attack – followed by financial losses (41%) and business and operational disruption (39%).

How did the cyber attack affect businesses in the Netherlands?
(Multiple answers were permitted)



FINDING 3: ORGANISATIONS IN THE NETHERLANDS ARE AWARE THAT THEY ARE AT RISK — BUT FACE CHALLENGES TO PROTECT THEMSELVES

Cyber risk and cyber preparedness is on most organisations' agenda, but often the reality is far from the desired state: when asked to what extent they thought their business was prepared for a cyber attack, 38% of respondents strongly felt that they are, with 46% somewhat agreeing.

When quizzed about the biggest risks to their organisation, Dutch CSOs/CISOs cited outdated or insufficient cybersecurity solutions and technology (67%), followed by human error and lack of security awareness (61%) and lack of proper access controls/processes (60%).

Given that threat actors increasingly target end-users, it's hardly surprising that IT leaders would consider human error and poor security awareness to be such a risk. What is surprising, is the lack of concern among board members about the cybersecurity posture of their organisations. Just 21% strongly agreed that cybersecurity was a board-level concern for their company in 2020.

Only 38% of CSOs/CISOs in the Netherlands strongly agree that their business is prepared for a cyber attack

To what extent do you agree or disagree with the following statements?*

	Strongly agree	Some-what agree	Neither agree nor disagree	Some-what disagree	Strongly disagree
 Our business is prepared for a cyber attack	38%	46%	7%	9%	0%
 Cybersecurity is a board-level concern for our company in 2020	21%	46%	21%	11%	0%
 Human error/lack of security awareness are the biggest risk for our organisation	32%	29%	32%	7%	0%
 Outdated or insufficient cybersecurity solutions/technology are the biggest risk for our organisation	26%	41%	18%	15%	1%
 Lack of proper access controls/processes is the biggest risk for our organisation	18%	42%	28%	12%	1%

*Due to rounding adjustments, some totals might not add up to 100%.

FINDING 4: DUTCH EMPLOYEES NEED TO BE BETTER EQUIPPED TO COMBAT CYBER ATTACKS

Despite end-users forming a last line of defence against cyber attacks, security knowledge and awareness is found to be lacking among the Dutch workforce.

Common security errors made by employees according to CSOs and CISOs in the Netherlands include mishandling sensitive information (53%), falling for phishing attacks (47%), insecure passwords (39%), sharing passwords (39%), criminal insider threats (34%) and clicking on malicious links (33%).

Proofpoint research has revealed that [almost one in four people who receive a phishing email will open it](#), with over 10% admitting to clicking on malicious links contained within.



Employee cyber awareness in the spotlight

With cyber attacks increasingly targeting people, it was surprising to see that 50% of Dutch CSOs/CISOs do not believe that their employees make their business vulnerable to a cyber attack.

Unfortunately, this sentiment is reflected in many Dutch organisations' cybersecurity awareness training programs, or lack thereof. Despite facing a fast-evolving threat landscape, 89% of CSOs/CISOs in the Netherlands admitted to training their employees on cybersecurity best practices as little as twice a year or less.

89% of CSOs/CISOs in the Netherlands admit to training their employees on cybersecurity best practices as little as twice a year or less.

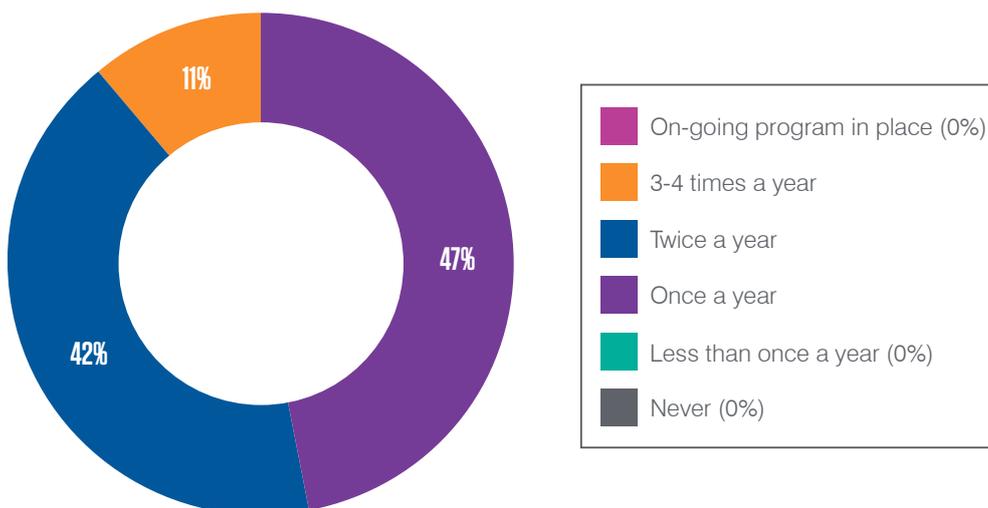
Do you think your employees make your business vulnerable to a cyber attack?

No 50%

Yes 50%

Regular and comprehensive training is vital to cybersecurity defence. All programs must be continually reviewed to ensure it remains relevant and keeps pace with the evolving threat landscape. Employee education and awareness of the latest threats is often the difference between an attempted cyber attack and a successful one. Failure to implement and review such programs leaves organisations dangerously exposed.

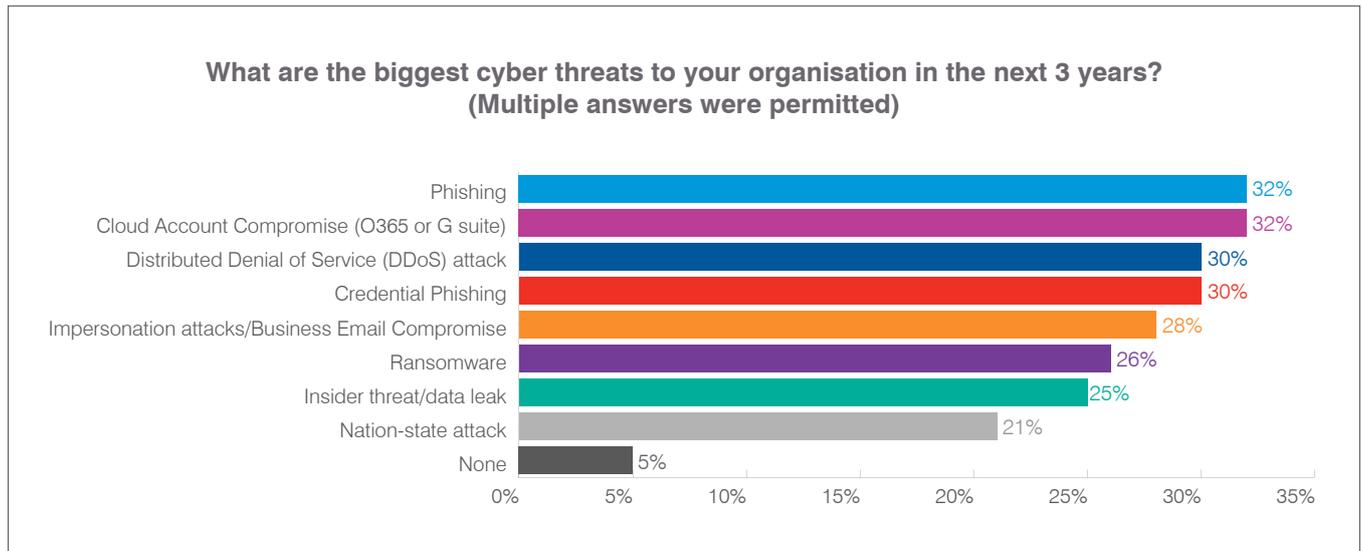
On average how often, if at all, do you train your employees on cybersecurity awareness/best practices?



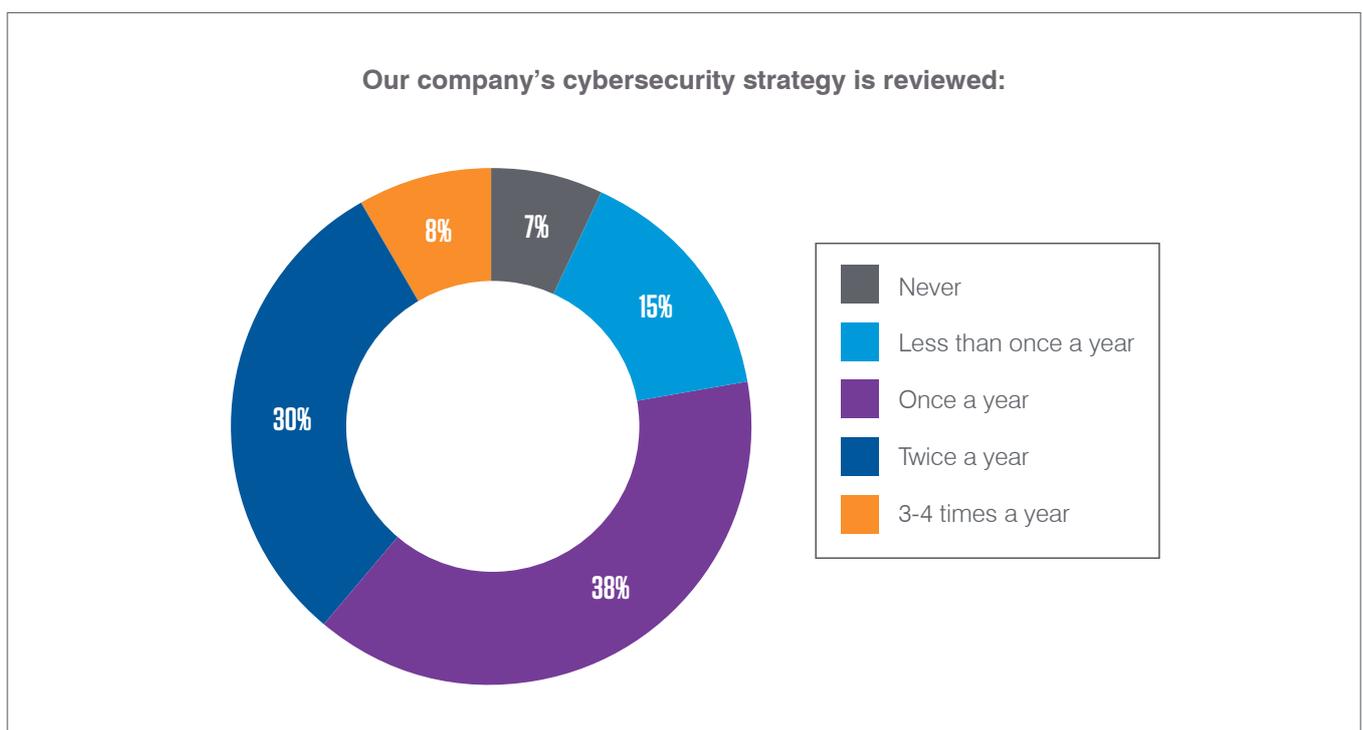
FINDING 5: THE FUTURE OF CYBER RISK IN THE NETHERLANDS IS SHIFTING

Evolving attack vectors and adapted cyber strategies

Looking forward to the next three years, 32% of Dutch CSOs/CISOs believe that phishing and cloud account compromise will continue to be the biggest cyber threats to their organisation in equal measures, followed by Distributed Denial of Service (DDoS) attacks (30%), credential phishing (30%), impersonation attacks or Business Email Compromise (28%), ransomware (26%), insider threats (25%) and finally, nation-state attacks (21%).



This evolving threat landscape calls for a shift in cyber defences, and constant re-assessment of an organisations' strategic priorities. Our survey revealed that 30% of CSOs/CISOs in the Netherlands review their cyber security strategy every six months with 38% reviewing once a year and 15% reviewing less than once a year. Shockingly, 7% never review their cyber security strategy.



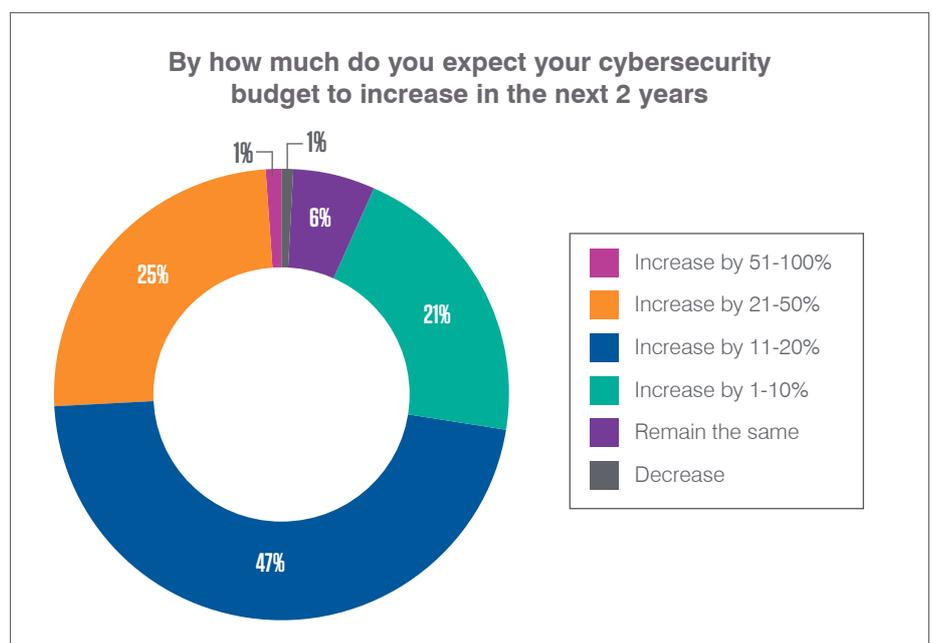
C-level awareness of cyber risk will drive technology investments

A gap in cybersecurity skills and training (44%) and a lack of awareness of cyber threats across the business (41%) were cited as the top two major obstacles to implementing cybersecurity technology by Dutch CSOs and CISOs. Other significant challenges include insufficient cybersecurity budgets (40%), and a lack of board-level buy-in (37%).

This leaves security teams in the difficult position of having to convince the C-suite of the calibre of the threats facing them in order to secure funding to implement preventative measures.



When it comes to cyber security investments over the next two years, our survey revealed that 73% of CSOs/CISOs in the Netherlands expect their cybersecurity budget to rise by 11% or more. This is a clear indicator that most organisations are aware of the need to improve cyber defences to reduce business risk exposure.



CONCLUSION

Irrespective of the means of attack – email, cloud applications, the web, social media – threat actors continue to take advantage of the human factor.

Whether it is impostors posing as trusted colleagues, or increasingly convincing phishing emails and malicious links, it is end-users who are on the frontline in the battle against cybercriminals.

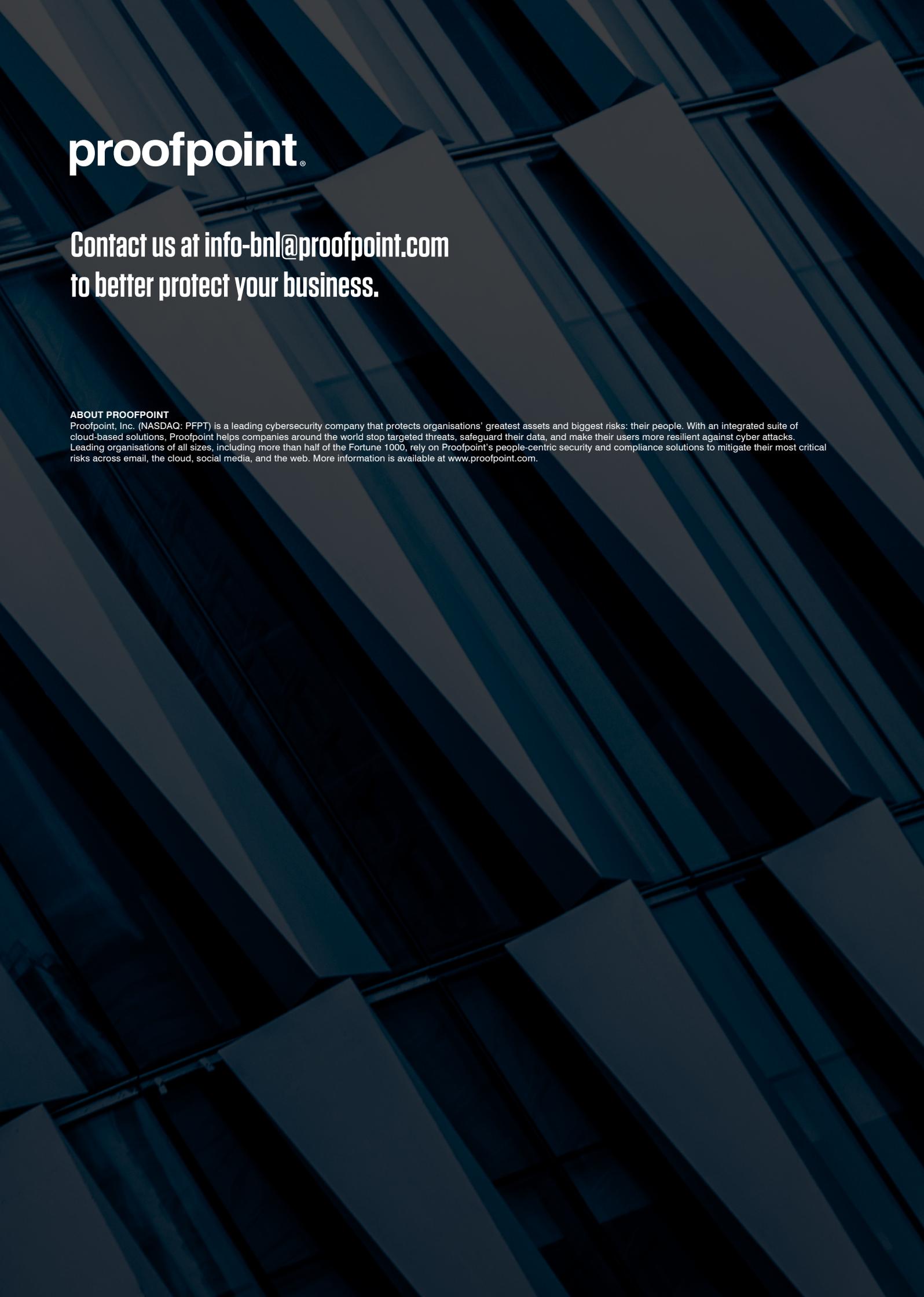
That's why a people-centric strategy is a must for organisations. This starts with identifying your most vulnerable users and ensuring they are equipped with the knowledge and the tools to defend your organisation.

Along with technical solutions and controls, a comprehensive security awareness training program must sit at the heart of your cyber defence. Training should be regular, comprehensive and adaptative and cover a range of topics – from the motivations and mechanics of cyber threats to how simple behaviours such as password reuse and inadequate data protection can increase the likelihood of a successful attack.

Cybercriminals are focused – forever honing their skills and techniques. If you're not doing the same, there can only be one winner.

Cybercriminals are focused – forever honing their skills and techniques. If you're not doing the same, there can only be one winner."

**Jim Cox, Regional Director,
Benelux for Proofpoint**



proofpoint®

**Contact us at info-bnl@proofpoint.com
to better protect your business.**

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint's people-centric security and compliance solutions to mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.