REPORT

PEOPLE-CENTRIC CYBERSECURITY:

A STUDY OF IT SECURITY LEADERS IN SWEDEN

EXECUTIVE SUMMARY

The cyber threat landscape in Sweden 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 Sweden. 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 Sweden experiencing at least one cyber attack in the past 12 months. From board level buy-in, to upping cybersecurity awareness training, organisations in Sweden 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 SWEDEN ARE FACING A DIVERSE THREAT LANDSCAPE

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

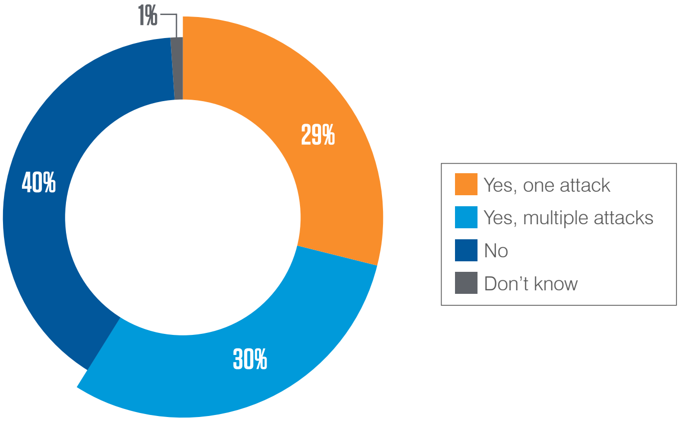
Our survey revealed that 59% of CSOs/CISOs said their company suffered at least one cyber attack in the past 12 months*. 30% said that their business was targeted multiple times.

Cybercriminals zone in on credentials

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 leading method of cyber attack in Sweden in the past year, impacting 43% of companies, followed by DDOS attacks (37%) and insider threat (33%).

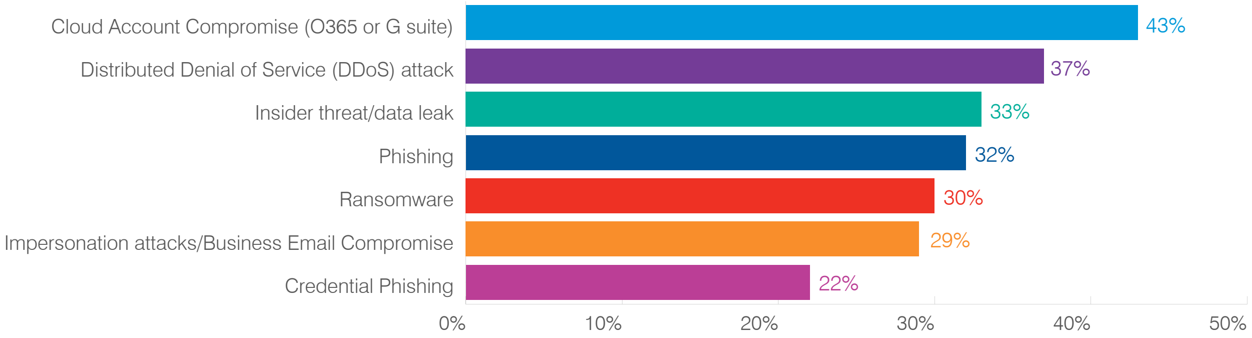
Did your organisation suffer a cyber attack in the past 12 months?



59% of organisations in Sweden suffered at least one cyber attack in the past 12 months.

Phishing attacks accounted for 32% and impersonation attacks for 29% amongst the Swedish organisations targeted last year. 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.

What type of cyber attack did your company suffer in the past 12 months (tick all that apply)?



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

FINDING 2: CSOS AND CISOS IN SWEDEN MOST CONCERNED ABOUT BRAND REPUTATION DAMAGE AND DATA BREACHES DUE TO CYBER ATTACKS

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

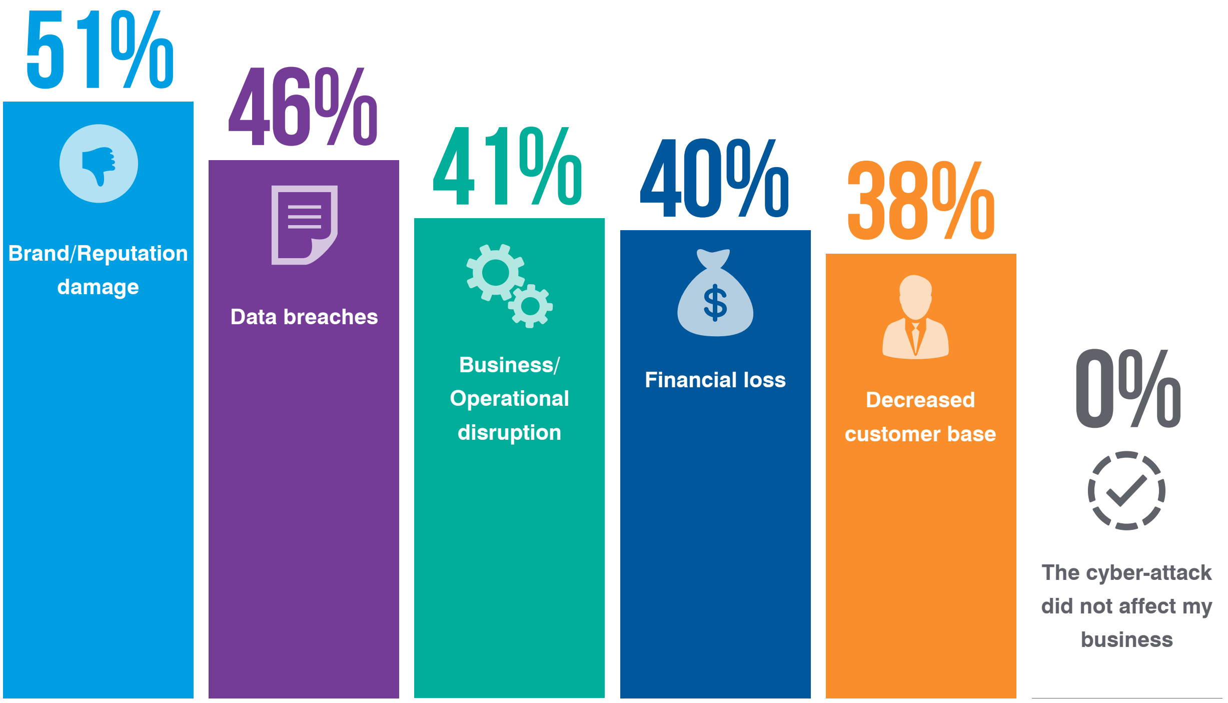
The World Economic Forum estimates that between 2019 and 2023, $5.2tr in global value will be at risk from malicious actors. From lost revenues and reputational damage to downtime, legal fees, compensation and remediation, the financial impact of such attacks can be far-reaching.

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 more than half (51%) of businesses in Sweden cited brand and reputation damage as the biggest consequence of a cyber attack – followed by data breaches (46%) and business and operational disruption (41%). Financial loss (40%) and decreased customer base (38%) are among the other common consequences cited.

51% of businesses in Sweden cited brand and reputation damage as the biggest consequence of a cyber attack – followed by data breaches (46%) and business and operational disruption (41%).

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



FINDING 3: ORGANISATIONS IN SWEDEN 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, only 29% of respondents strongly felt that they are, with 50% somewhat agreeing.

When quizzed about the biggest risks to their organisation, Swedish CSOs/CISOs cited outdated or insufficient cybersecurity solutions and technology (49%), followed by lack of proper access controls/processes (47%) and human error and lack of security awareness (46%).

Only 29% of CSOs/CISOs in Sweden strongly agree that their business is prepared for a cyber attack

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 24% strongly agreed that cybersecurity was a board-level concern for their company in 2020.

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

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Our business is prepared for a cyber attack	29%	50%	14%	6%	1%
Cybersecurity is a board-level concern for our company in 2020	24%	36%	29%	11%	1%
Human error/lack of security awareness are the biggest risk for our organisation	15%	31%	28%	19%	6%
Outdated or insufficient cybersecurity solutions/technology are the biggest risk for our organisation	14%	35%	25%	20%	6%
Lack of proper access controls/processes is the biggest risk for our organisation	13%	34%	27%	18%	7%

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

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

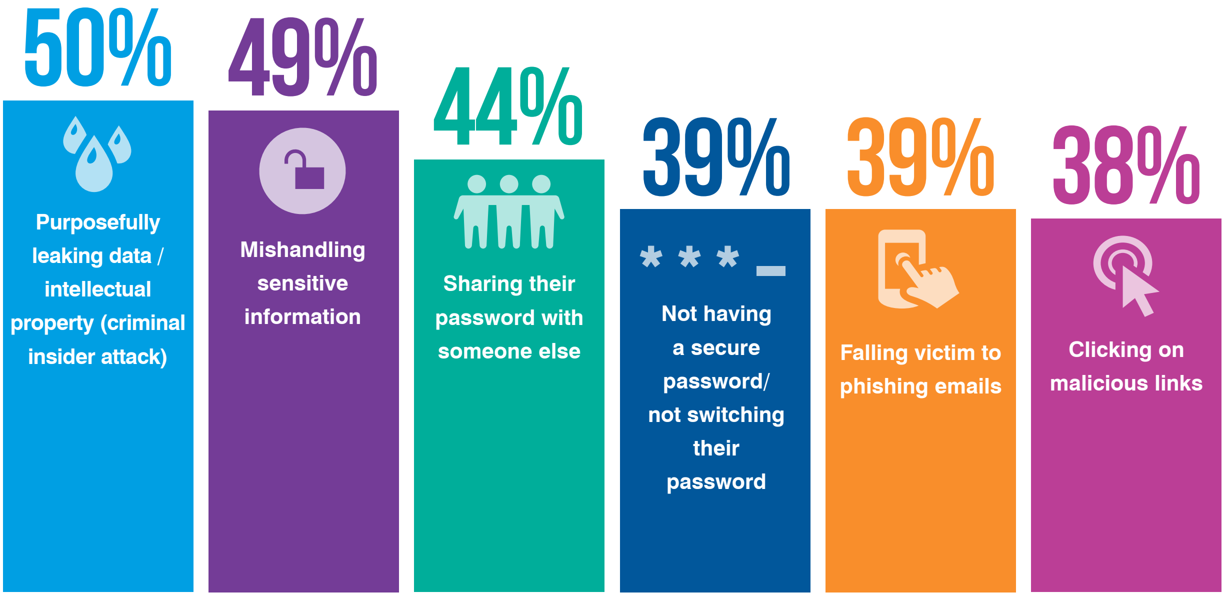
Despite end-users forming a last line of defence against cyber attacks, security knowledge and awareness is found to be lacking among Sweden's workforce.

Common ways CSOs/CISOs in Sweden think their employees make their business vulnerable to a cyber-attack include mishandling of sensitive information (49%), poor password hygiene (44%) and falling victim to phishing attacks (39%) and clicking on malicious links (38%).

Insider threats on the rise

Interestingly, a staggering 50% of CSOs/CISOs said that purposefully leaking data or intellectual property (also known as criminal insider threat) was putting their business at risk. 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.

Ways in which Swedish employees make their business vulnerable to cyber attacks



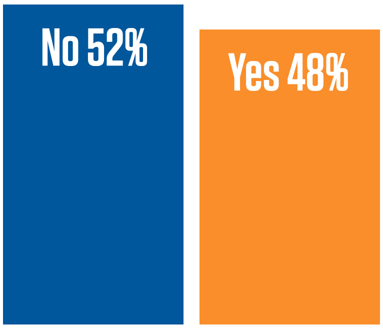
Employee cyber awareness in the spotlight

With cyber attacks increasingly targeting people, it was surprising to see that 52% of Swedish CSOs/CISOs do not believe that their employees make their business vulnerable to a cyber attack.

Unfortunately, this sentiment is reflected in many Swedish organisations' cybersecurity awareness training programs, or lack thereof. Despite facing a fast-evolving threat landscape, three-quarters (76%) of CSOs/CISOs in Sweden admitted to training their employees on cybersecurity best practices as little as twice a year or less, with 6% saying they never do.

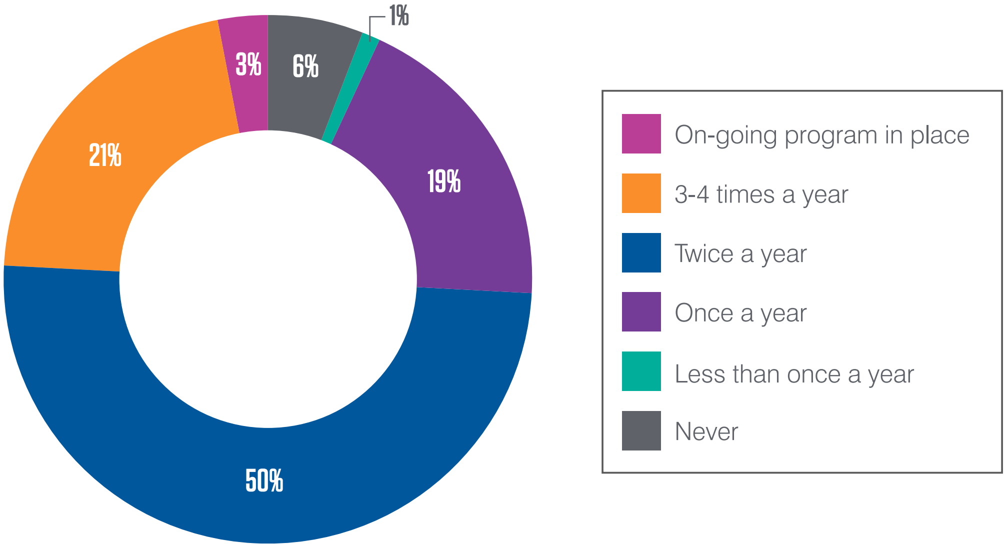
(76%) of CSOs/CISOs in Sweden admitted to training their employees on cybersecurity best practices as little as twice a year or less.

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



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?

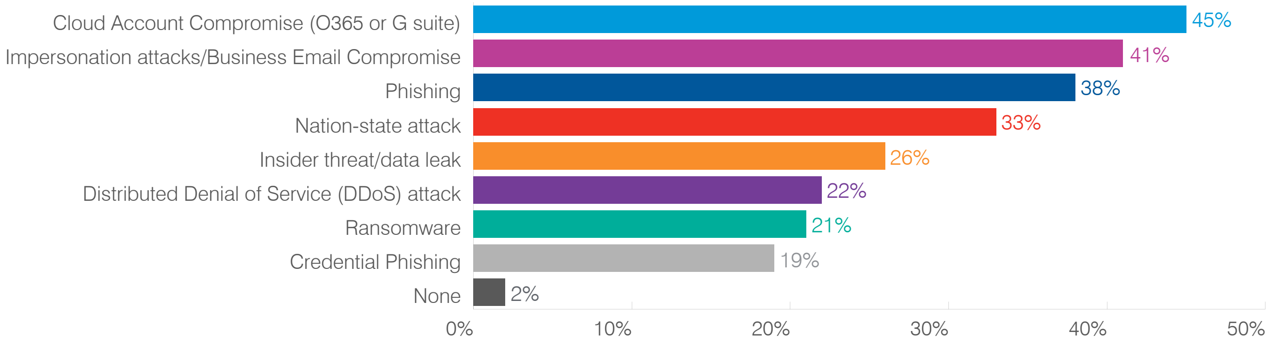


FINDING 5: THE FUTURE OF CYBER RISK IN SWEDEN IS SHIFTING

Evolving attack vectors and adapted cyber strategies

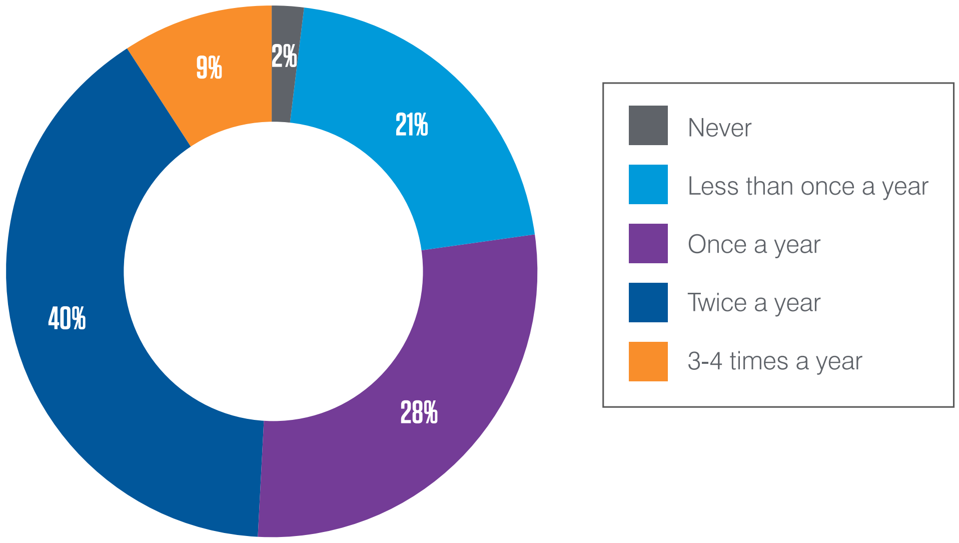
Looking forward to the next three years, 45% of Swedish CSOs/CISOs believe that cloud account compromise will continue to be the biggest cyber threat to their organisation, followed by impersonation attacks or Business Email Compromise (41%), phishing (38%), nation-state attacks (33%), insider threats (26%), Distributed Denial of Service (DDoS) attack (22%), Ransomware (21%) and finally credential phishing (19%).

What are the biggest cyber threats to your organisation in the next 3 years? (Multiple answers were permitted)



This evolving threat landscape calls for a shift in cyber defences, and constant re-assessment of an organisations' strategic priorities. Our survey revealed that 40% of CSOs/CISOs review their cyber security strategy every six months with 28% reviewing once a year and 21% reviewing less than once a year.

Our company's cybersecurity strategy is reviewed:

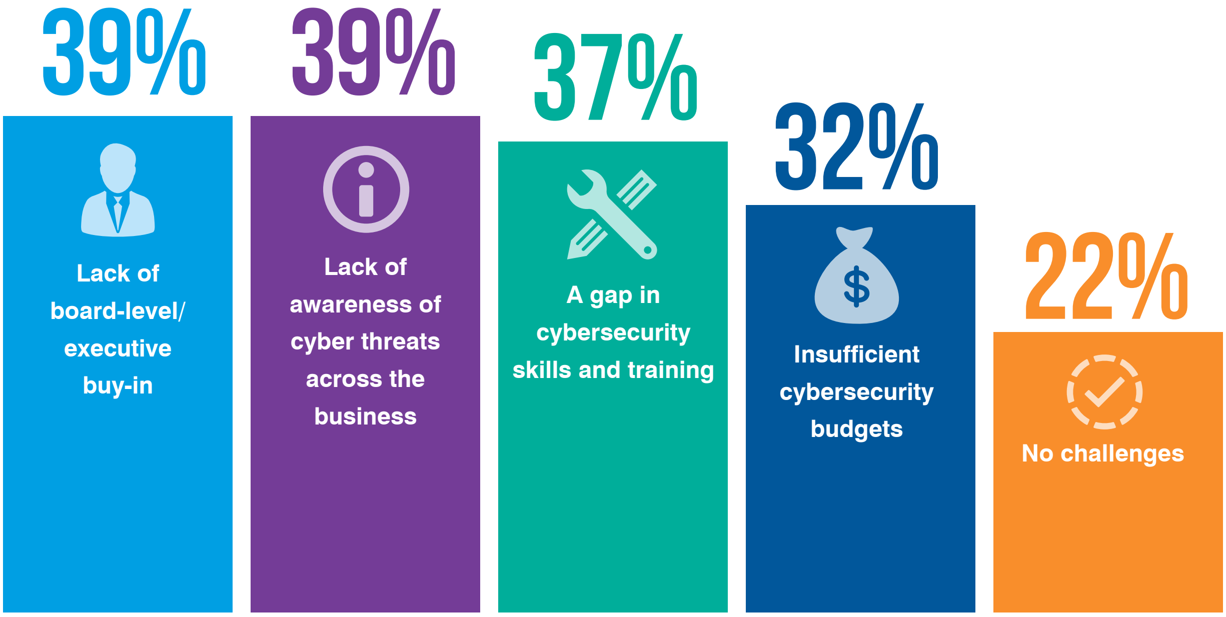


C-level awareness of cyber risk will drive technology investments

A lack of awareness of cyber threats across the business and a lack of board-level buy-in were cited in equal measure as major obstacles to implementing cybersecurity technology by 39% of Swedish CSOs and CISOs. Other significant challenges include gap in cybersecurity skills and training (37%) and insufficient cybersecurity budgets (32%).

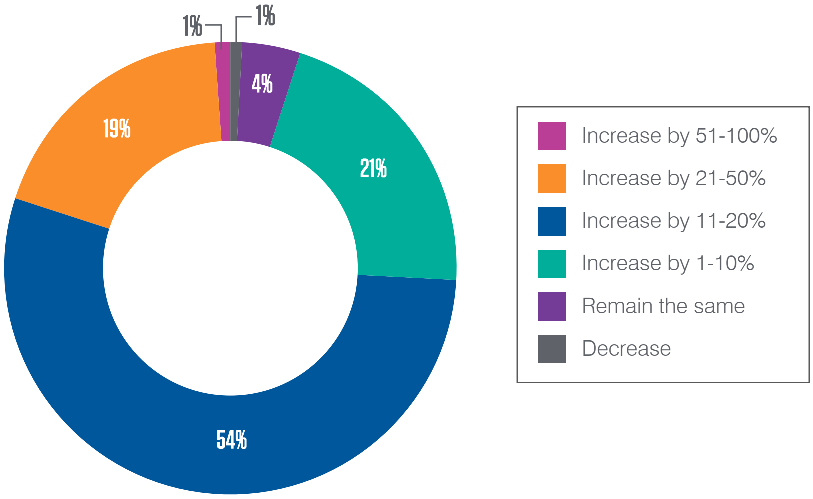
This leaves security teams in the difficult position of having to convince the C-suite of the calibre of the threats facing them in order to secure funding to implement preventative measures.

Biggest challenges faced by organisations in Sweden when implementing cybersecurity technology (Multiple answers were permitted)



When it comes to cyber security investments over the next two years, our survey revealed that 74% of CSOs/CISOs in Sweden 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.

By how much do you expect your cybersecurity budget to increase in the next 2 years



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."*
>
> **Örjan Westman, Regional Director, Nordics for Proofpoint**

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

All data unless specified otherwise is in reference to the research conducted by Censuswide, with 150 CSO/CISOs in the Sweden between 04.03.2020 - 11.03.2020. Censuswide abide by and employ members of the Market Research Society which is based on the ESOMAR principles.

proofpoint.

Contact us at info-nor@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.