

proofpoint®

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

## EXECUTIVE SUMMARY

The cyber threat landscape in the United Arab Emirates (UAE) 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 can 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 unauthorized applications.

To address this, organizations 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 organizations, Proofpoint commissioned a survey of 150 CSOs/CISOs across the UAE. The study, conducted by research firm Censurwide, surveyed CSOs/CISOs in the UAE with a natural fallout across industries in March 2020.

### **The study explored three key areas:**

- Frequency of cyber attacks
- Employee and organizational 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 organizations in the UAE experiencing at least one cyber attack in 2019. From board level buy-in, to upping cybersecurity awareness training, organizations in the UAE are taking steps to shore up their cyber defenses.

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

## FINDING 1: ORGANIZATIONS IN THE UAE ARE FACING A DIVERSE THREAT LANDSCAPE

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

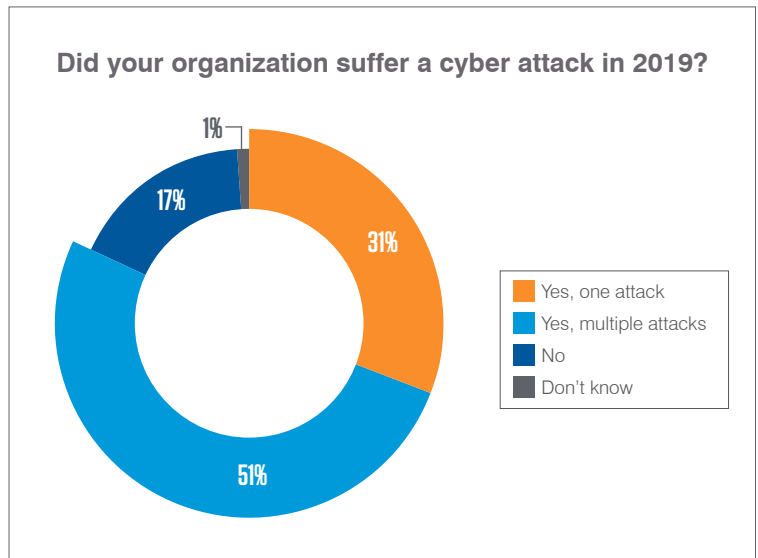
Our survey revealed that 82% of CSOs/CISOs said their company had suffered at least one cyber attack in 2019\*. Over half (51%) reported multiple incidents and almost a third (31%) experienced one.

### Cybercriminals zone in on credentials

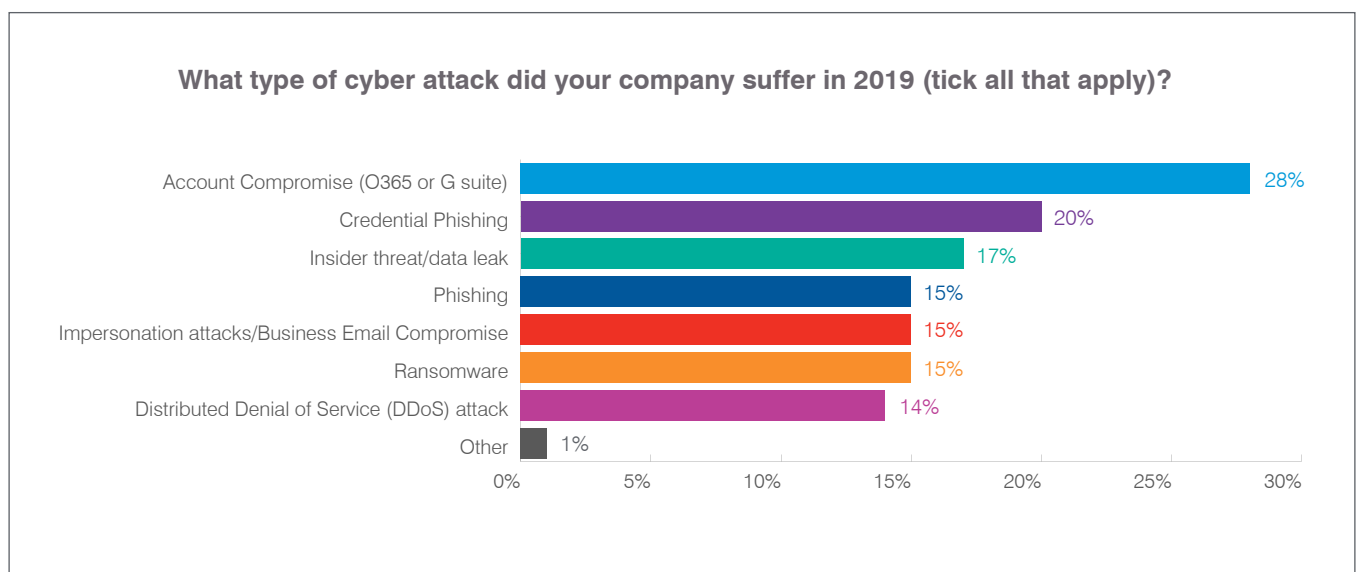
Cybercriminals are increasingly using compromised credentials to access email accounts, sensitive information and corporate systems. Credentials are often phished via email – a method of attack that remains alarmingly effective.

Our research found that account compromise was the leading method of cyber attack in the UAE in 2019, impacting 28% of companies, followed by credential phishing (20%) and insider threats (17%).

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. Phishing and impersonations attacks each accounted for 15% amongst the organizations targeted last year.



*82% of organizations in the UAE suffered at least one cyber attack in 2019*



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

## FINDING 2: CSOS AND CISOS IN THE UAE MOST CONCERNED ABOUT FINANCIAL LOSS AND DATA BREACHES DUE TO CYBER ATTACKS

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

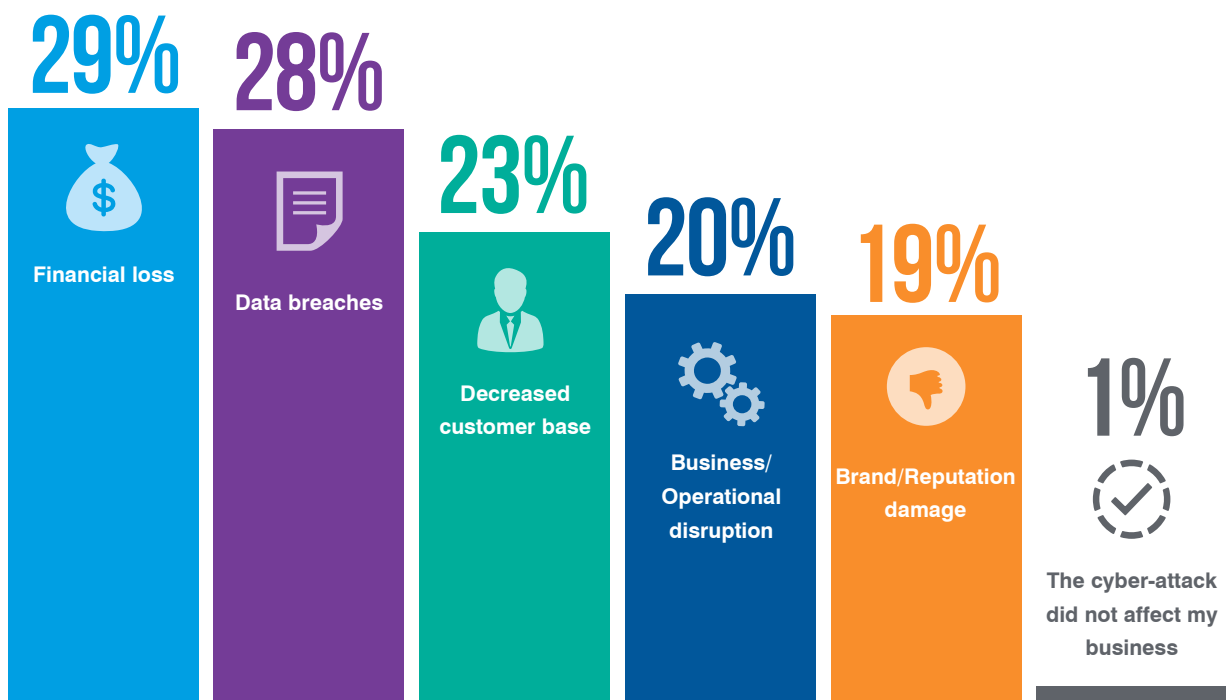
The World Economic Forum estimates that between 2019 and 2023, [\\$5.2tr in global value will be at risk](#) from malicious actors. From lost revenues and reputational damage to downtime, legal fees, compensation and remediation, the financial impact of such attacks can be far-reaching.

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 almost a third (29%) of companies in the UAE cited financial loss as the biggest consequence of a cyber attack – followed by data breaches (28%) and decreased customer base (23%). Business and operational disruption (20%) and damage to reputation (19%) are among the other common consequences cited.

*29% of companies in the UAE cited financial loss as the biggest consequence of a cyber attack – followed by data breaches (28%) and decreased customer base (23%).*

How did cyber attacks affect UAE businesses? (Multiple answers were permitted)



## FINDING 3: ORGANIZATIONS IN THE UAE ARE AWARE THEY ARE AT RISK - BUT FACE CHALLENGES TO PROTECT THEMSELVES






Cyber risk and cyber preparedness are on most organizations' 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 21% of respondents strongly felt that they were, and 43% were somewhat in agreement.

When quizzed about the biggest risks to their organization, CSOs/CISOs cited outdated or insufficient cybersecurity solutions and technology (59%), followed by human error and lack of security awareness (55%) and lack of proper access controls/processes (55%).

Given that threat actors increasingly target end-users, it's hardly surprising that IT security 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 organizations. Just 21% strongly agreed that cybersecurity is a board-level concern for their company in 2020.

*Only 21% of CSOs/CISOs in the UAE 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	21%	43%	34%	2%	1%
 Cybersecurity is a board-level concern for our company in 2020	21%	48%	29%	1%	1%
 Human error/lack of security awareness are the biggest risk for our organization	16%	39%	34%	10%	1%
 Outdated or insufficient cybersecurity solutions/technology are the biggest risk for our organization	17%	42%	29%	10%	2%
 Lack of proper access controls/processes is the biggest risk for our organization	17%	38%	34%	8%	3%

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



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

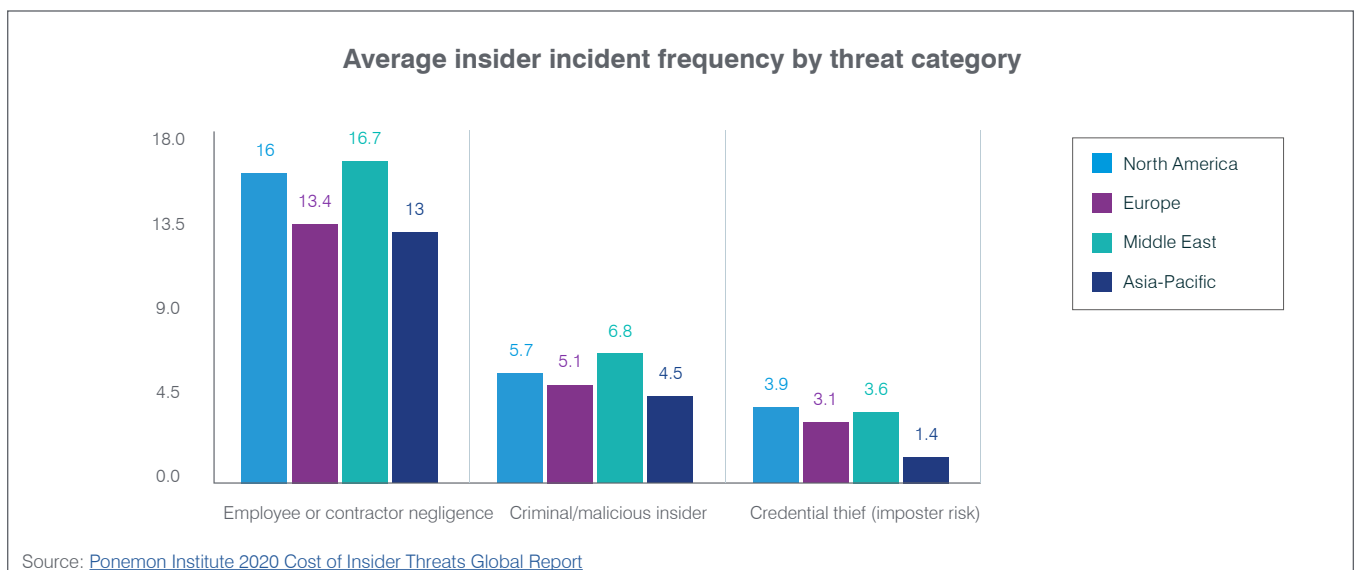
Despite end-users forming a last line of defense against cyber attacks, security knowledge and awareness is found to be lacking among the UAE's workforce.

Common ways CSOs/CISOs in the UAE think their employees make their business vulnerable to a cyber-attack include poor password hygiene (29%), mishandling of sensitive information (25%), falling victim to phishing attacks (24%), and clicking on malicious links (20%).



### Insider threats on the rise

Interestingly, 19% of CSOs/CISOs in the UAE said that employees purposefully leaking data or intellectual property (also known as criminal insider threat) was making their business vulnerable to a cyber-attack. Insider threats are a growing concern for businesses, with the number of incidents up [by a staggering 47 percent in just two years](#).



The 2020 Ponemon Institute [Cost of Insider Threats report](#) shows that companies in the Middle East experienced the most insider incidents and are most likely to experience credential theft compared to other regions in the last year.

## Employee cyber awareness in the spotlight

With cyber attacks increasingly targeting people, it was surprising to see that 61% of CSOs/CISOs in the UAE do not believe that their employees make their business vulnerable to a cyber attack.

Unfortunately, this sentiment is reflected in many UAE organizations' cybersecurity awareness training programs, or lack thereof. Despite facing a fast-evolving threat landscape, three-quarters (75%) of CSOs/CISOs in the UAE admitted to training their employees on cybersecurity best practices as little as twice a year or less, with 23% running a comprehensive program three times a year or more.

*75% of organizations in the UAE admitted to training their employees on cybersecurity best practices as little as twice a year or less.*

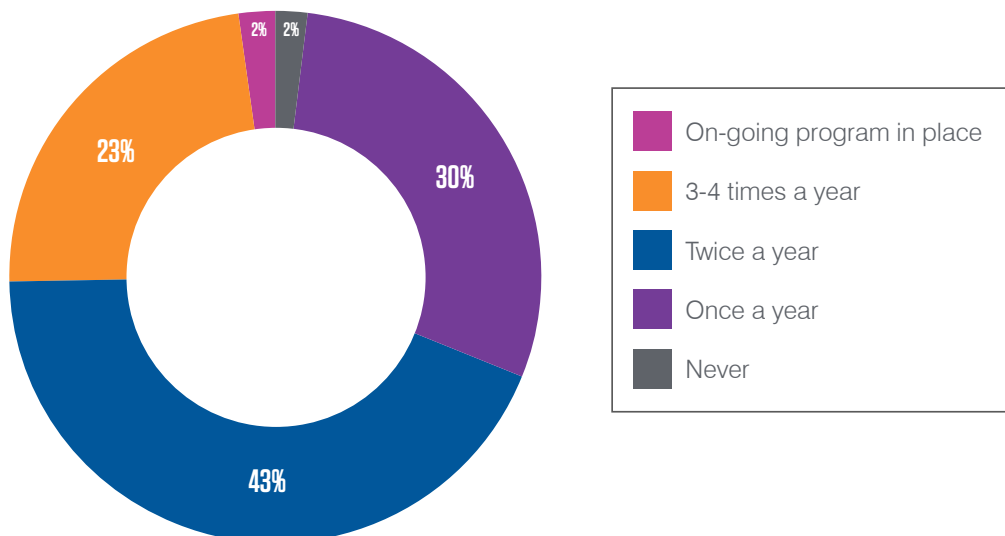
**Do you think your employees make your business vulnerable to a cyber-attack?**

**No 61%**

**Yes 39%**

Regular and comprehensive training is vital to cybersecurity defense. All programs must be continually reviewed to ensure they remain relevant and keep 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 organizations dangerously exposed.

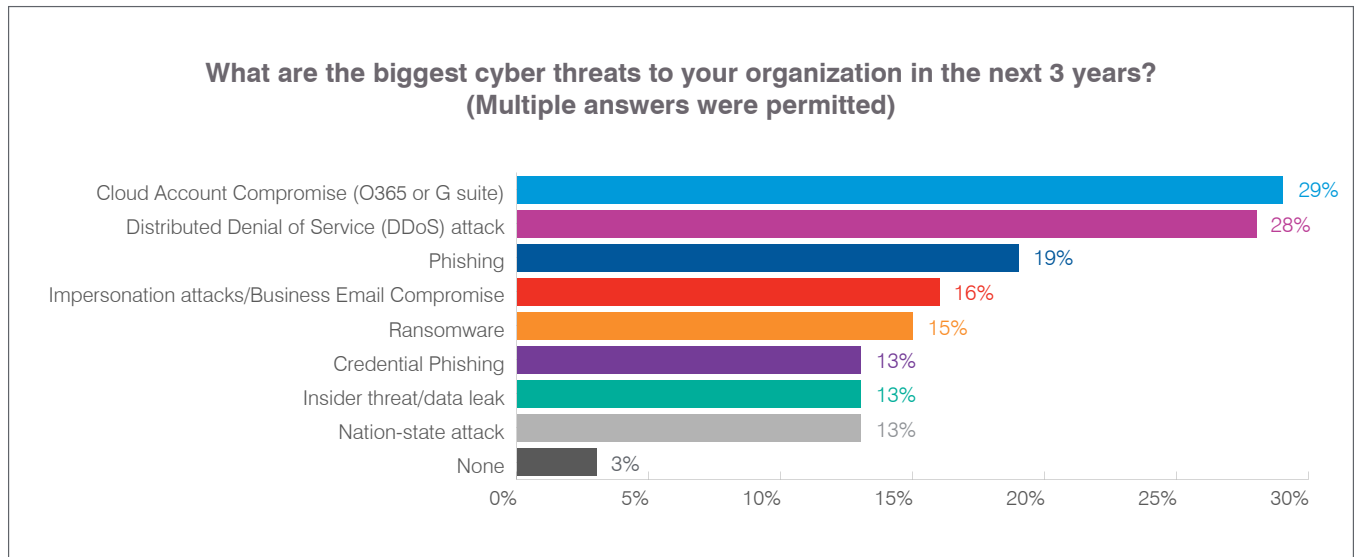
**On average how often, if at all, do you train your employees on cybersecurity awareness/best practices?**



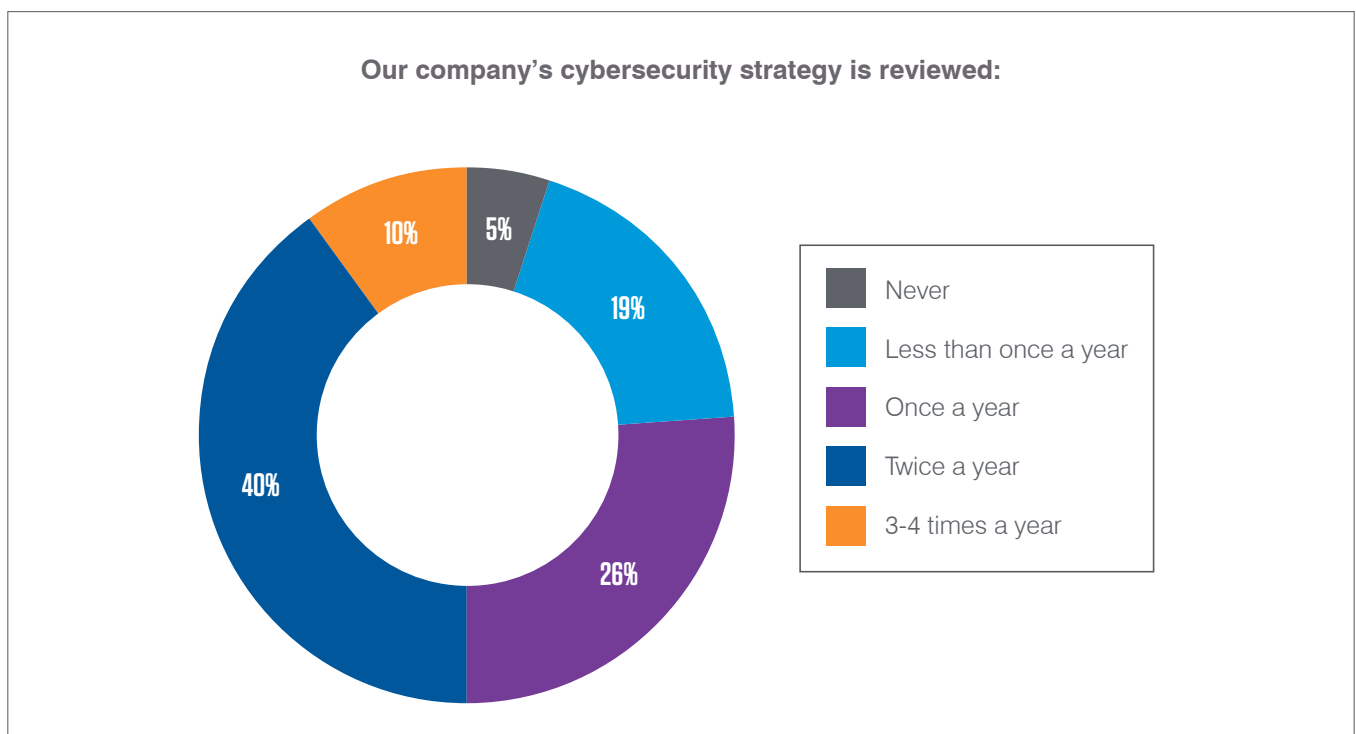
## FINDING 5: THE FUTURE OF CYBER RISK IN THE UAE IS SHIFTING

### Evolving attack vectors and adapted cyber strategies

Looking forward to the next three years, almost a third (29%) of respondents believe that account compromise will continue to be the biggest cyber threat within their industry in the next 3 years, followed by Distributed Denial of Service (or DDoS) attacks (28%), phishing (19%), impersonation attacks/ Business Email Compromise (BEC) (16%), ransomware (15%), credential phishing (13%), insider threat/data leak (13%) and nation-state attacks (13%).



This evolving threat landscape calls for a shift in cyber defenses, and constant re-assessment of an organization's strategic priorities. Our survey revealed that 40% of CSOs/CISOs in the UAE review their cybersecurity strategy twice a year with 26% reviewing once a year and 19% reviewing less than once a year.





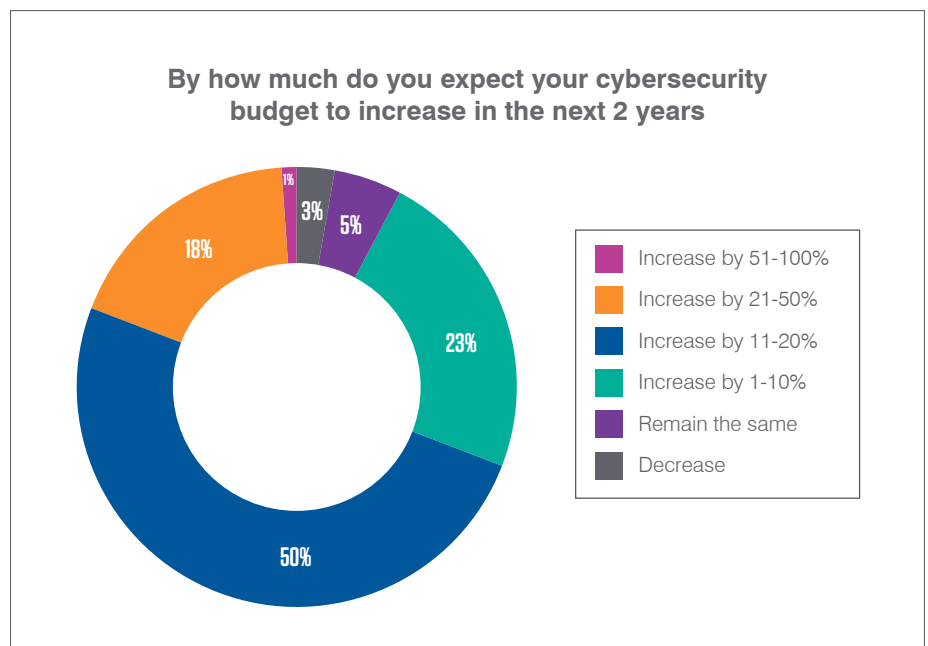
## C-level awareness of cyber risk will drive technology investments

A lack of board-level buy-in was cited as a major obstacle to implementing cybersecurity technology by 31% of CSOs/CISOs in the UAE. Other significant challenges include a lack of awareness of cyber threats across their business (29%) and insufficient cybersecurity budgets (23%).

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



When it comes to cybersecurity investments over the next two years, our survey revealed that 69% of CSOs/CISOs in the UAE expect their cybersecurity budget to rise by 11% or more. This is a clear indicator that most organizations are aware of the need to improve cyber defenses 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 organizations. This starts with identifying your most vulnerable users and ensuring they are equipped with the knowledge and the tools to defend your organization.

Along with technical solutions and controls, a comprehensive security awareness training program must sit at the heart of your cyber defense. Training should be regular, comprehensive and adaptative and cover a range of topics – from the motivations and mechanics of cyber threats to how simple behaviors 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.”*

**Emile Abou Saleh, Regional Director, Middle East and Africa for Proofpoint**

# proofpoint®

## ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' 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 organizations 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](http://www.proofpoint.com).