proofpoint.

REPORT

UNDERSTANDING EMAIL FRAUD

A GLOBAL SURVEY OF IT LEADERS IN THE US, THE UK, AUSTRALIA, FRANCE, AND GERMANY

proofpoint.com

Email fraud, also known as Business Email Compromise (BEC), is one of today's greatest cyber threats. These socially engineered attacks seek to exploit people rather than technology. They are highly targeted, don't include attachments or URLs, arrive in low volumes, and impersonate people in authority. These and other factors make email fraud difficult to detect and stop with traditional security tools.

Email fraud preys on human nature — fear, the desire to please, and more– to steal money and valuable information from employees, customers, and business partners. To better understand how email fraud is affecting the companies targeted by it, Proofpoint commissioned a survey of more than 2,250 IT decision makers across the U.S., the U.K., Australia, France, and Germany.

The survey, conducted by research firm Censuswide, ran Jan. 6–18, 2018. It included companies with 200 or more people across a range of industries. More than 500 people in each country took part (except Australia, where 250 did the survey). For additional insight, we also drew on data from our threat research team, which has analysed more than 160 billion emails.

We explored three key questions:

- How are businesses affected?
- Who is most at risk?
- How are companies protecting themselves, if at all?

The answers are revealing. We found that email fraud is pervasive, disruptive, and in many cases, catching businesses unprepared. Just 40% of survey respondents say they have full visibility into email fraud threats in their environment, and even fewer have controls in place to stop them.

This report highlights these and other results of the survey.

FINDING 1: EMAIL FRAUD IS SOARING

Email fraud, which spans a range of attacks and techniques, was rife in 2017. These attacks usually start with an email or series of emails purporting to come from a top executive or business partner. The email asks the recipient to wire money or send sensitive information. It does not use malicious attachments or URLs, so it can be hard to detect and stop.

Email fraud can ensnare even sophisticated victims. In just one example, a Lithuanian man is accused of stealing more than $100 million in separate attacks on Google and Facebook in July 2017[1]. The man allegedly spoofed a vendor in the companies' supply chains.

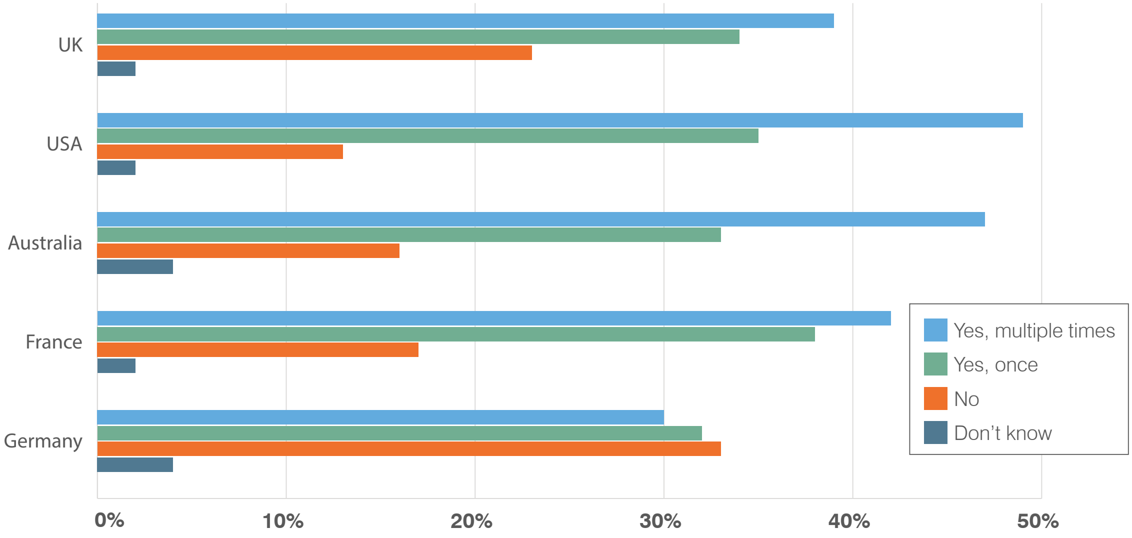
MOST COMPANIES TARGETED

While the threat continues to be highly targeted, attacks were launched against more organizations and with greater frequency than in 2016. According to our threat research team, the percentage of companies targeted by at least one email fraud attack has steadily risen, reaching a new high of 88.8% in Q4 2017[2].

The Censuswide survey was in line with that figure. About 75% of organisations said they were targeted at least once by email fraud attacks in the last two years. More than 2 in 5 (41%) said that their business has been targeted multiple times.

Germany appears to be the least targeted country. Nearly 63% said they were targeted by one or more email fraud attacks in the previous two years. The U.S. is the most targeted, with 84% reporting one or more attacks. Australia came in second at nearly 80%. We have found no correlation between the size of business and the likeliness of attack. In other words, all businesses are at risk.

Has your business been targeted with Business Email Compromise attacks in the last 2 years?



GROWING AWARENESS

As companies become more aware of email fraud, a growing number expect to see such attacks targeted at them. Overall, 77% of respondents said their company was "likely" or "very likely" to be targeted by email fraud in the next year. U.S. companies are most affected, with 83.4% expecting an attack.

German companies are least affected, with just 66.4% expecting an attack. In both cases, the percentage is close to the number reporting actual attacks in the two previous years.

Despite a growing awareness of the threat, 1 in 7 respondents said they don't think their company will be targeted in the next year.

[1] Reuters. "Lithuanian court upholds extradition of man to U.S. in $100 million fraud case." August 2017.
[2] Proofpoint. "Email Fraud Threat Report: Year in Review." February 2018.

FINDING 2: EMAIL FRAUD HAS A BIG IMPACT ON VICTIMS

The effects of email fraud are not always immediate but are usually severe. In addition to direct financial losses, which can be substantial, email fraud can disrupt business, result in loss of data, and lead to firing of those in high-level positions.

BUSINESS, DISRUPTED

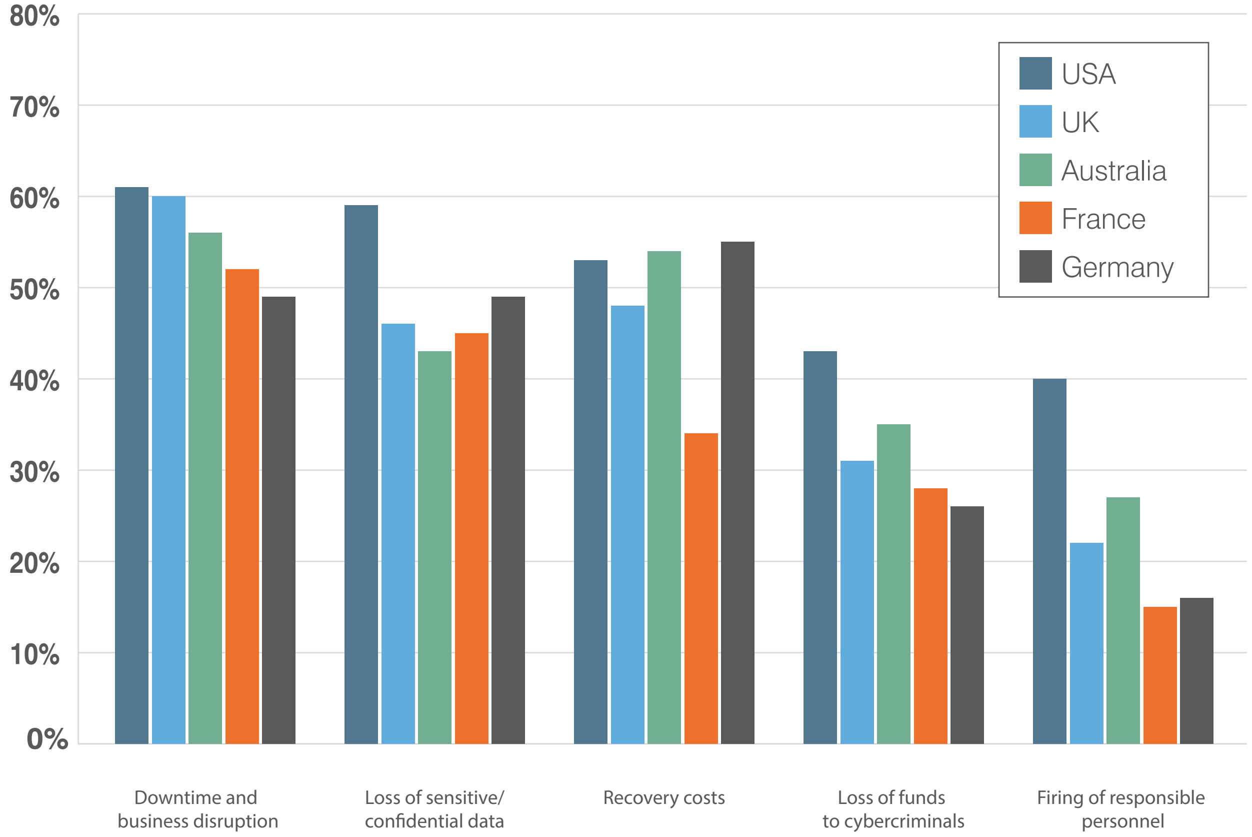
Business disruption was the most common effect, according to 55.7% of survey participants who were hit by an email fraud attack. The finance sector was hit the hardest, with 63% of email fraud attacks disrupting business. Geographically, U.S. companies suffered business disruption the most often at 61%, and Germany suffered the least, often at just 49%.

In a third of email fraud attacks, the cyber criminal tricked the victim into sending money. In about half of all cases, the company lost sensitive data.

In nearly 1 in 4 attacks, someone was fired for letting it happen. U.S. companies were the most likely to sack the person deemed responsible in 40% of all cases. France, with its stringent employment laws, was least likely to do so.

> *Business disruption was the most common effect, according to 55.7% of survey participants who were hit by an email fraud attack.*

What was the impact of the email attacks on your business in the last 2 years?



REACHING FURTHER DOWN THE ORG CHART

Cybercriminals have moved beyond CEO-to-CFO spoofing, where they pretend to be the chief executive to trick the finance leader into wiring money. Now they're impersonating more identities and targeting a wider range of people within the targeted organisation.

After holding steady for the first three quarters of 2017, the average number of identities spoofed per organisation more than doubled in Q4 to about 10 identities, according to our threat research[3].

Companies are noticing a similar trend. In the Censuswide survey, more than half (55%) of respondents said their finance team is most at risk of email fraud. That's no surprise — attackers follow the money. But 43% of respondents also see accounts payable as a potential target, followed by the C-suites (37%), and the general workforce (33%).

Who in your organisation do you consider most at risk of receiving fake emails impersonating someone within your business?

	Finance Team	Accounts Payable	C-suites	General Workforce
🇺🇸	62%	52%	44%	36%
🇬🇧	57%	50%	30%	33%
🇦🇺	56%	50%	26%	33%
🇩🇪	61%	36%	28%	31%
🇫🇷	38%	32%	52%	32%

U.S. firms appear to be most aware, reporting the highest concerns of risk across all of the employee groupings in the survey. They, too, see the finance team as being most at risk (62%), as do their German counterparts (61%). French companies are twice as likely to view their C-suites as potential targets (52%) as those in Australia (26%) and Germany (28%).

[3] Proofpoint. "Email Fraud Threat Report: Year in Review." February 2018.

FINDING 3: EMAIL FRAUD IS A BOARD-LEVEL ISSUE

Email fraud is a business risk, not just an IT issue.

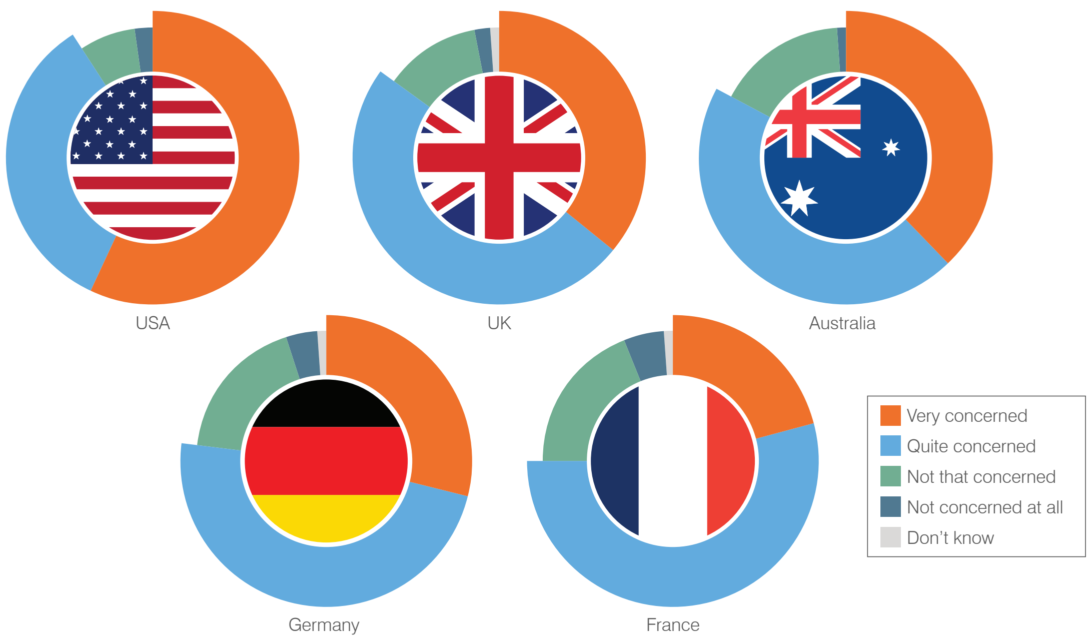
With the World Economic Forum[4] ranking cyberattacks and data breaches second only to natural disasters and extreme weather in terms of risk, cyber threats are a priority businesses can no longer ignore.

EMAIL FRAUD IS A PRIORITY...

The good news: email fraud has caught the attention of top leadership. A large majority of survey respondents (82%) said the threat is a concern for board members and executive teams.

Interestingly, U.S. companies are more likely to call email fraud a board-level issue (91%) in comparision to those in Germany and France (76.8% and 74.6%, respectively).

How concerned are your board and executive teams with email fraud attacks to the business?



More than half of those surveyed (59%) consider email fraud one of the top security risks to their businesses. And 86% called it an IT security priority for their organisation.

The industries most likely to list email fraud as a top IT security priority include professional services (92%), IT and telecommunications (90%), and finance (88%).

...BUT NOT EVERYONE IS PREPARED FOR IT

We found striking differences in what companies are doing to combat email fraud.

Overall, less than half of the companies surveyed had used available technology to protect themselves against email fraud (such as email authentication). The U.S. led with 60% adoption—well ahead of the curve. On the other end of the spectrum, only 32% of German respondents said the same.

[4] World Economic Forum. "The Global Risks Report 2018". January 2018.

HOW ORGANISATIONS ARE RESPONDING

Email fraud is more pervasive and sophisticated than ever. You can't rely on static anti-spoofing policies and traditional security tools to stop it. To understand how organisations are protecting themselves, we looked at three factors that are core to an effective, multi-layered defence: people, process, and technology.

PEOPLE

57%

of respondents have an end-user awareness programme on phishing in place

PEOPLE

More than half (57%) of those polled have an end-user awareness programme on phishing in place, and 32% plan to introduce one in 2018.

The U.S. is ahead of the curve with 67% of companies already offering such training. Germany is last with only 50% of companies offering it.

Among industries, 66% of finance and professional services companies train employees on spotting phishing emails. But alarmingly, only half of the healthcare companies surveyed did the same — despite being one of cybercriminals' favourite targets.

PROCESS

62%

of respondents admitted they don't have financial controls in place to stop wire transfer fraud

23%

said their business has purchased cyber insurance to cover email fraud risks

PROCESS

On the process front, there is still much more to be done.

Nearly a third (33%) of targeted organisations have lost funds to cybercriminals. And yet more than 3 in 5 (62%) of respondents admitted they don't have financial controls in place to stop such attacks. Germany was most at risk; more than two-thirds (67%) were lacking wire-transfer controls.

TECHNOLOGY

46%

of respondents have used an email authentification system

56%

do not have user-access levels in place for systems used to process personal data

55%

do not have end-to-end email encryption for sensitive data in place

TECHNOLOGY

We surveyed companies with regard to their email authentification protocols, end-to-end email encryption, and user-access level controls for systems that process sensitive data.

EMAIL AUTHENTICATION

Email authentication is an essential first step to protecting yourself against email fraud. This includes Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC). Used in combination, these protocols can stop email domain spoofing which is used in many email fraud attacks. Just under half (46%) of those surveyed have deployed email authentication protocols and 37% are planning to do so this year.

Yet, only 40% say they have complete visibility into domain spoofing threats and control over their own email domains. A worrying fact when our threat research shows that 93% of companies were targeted with domain spoofing attacks in 2017[5].

Some countries had better visibility into their email ecosystem than others. In the U.S., more than half (55%) of respondents claim they have full visibility; the highest percentage among countries surveyed. The fact that this is higher in the U.S. makes sense, given its high adoption rates of email authentication protocols. At the other end of the spectrum, only 29.6% of respondents in France said they have full visibility.

Most companies (93%) recognise that email fraud is a multifaceted problem: cybercriminals spoof not just the targeted company's domain but those of its partners and suppliers, too. Nearly half of respondents said they've created policies requiring external business partners to protect their supply chain.

46%

of respondents have deployed email authentication protocols and 37% are planning to do so this year

DATA PROTECTION

According to the 2017 Verizon Data Breach Investigations Report, more than 80% of data breaches happen as a result of cybercriminals stealing data. However, according to our survey, 56% of respondents said they do not have user-access levels in place for systems that are used to process personal data.

Meanwhile, 55% of businesses do not have end-to-end email encryption for sensitive data in place; a rather worrying fact in light of the General Data Protection Regulation (GDPR) requirements.

55%

of businesses do not have end to end email encryption for sensitive data in place

TRANSFERRING RISK

Our survey found that some organisations have opted to transfer risk. Nearly one fourth of respondents (23%) said their business has purchased cyber insurance to cover email fraud risks.

Cyber insurance can help cushion the cost of email fraud. But the cyber insurance market is still under prepared. In some cases, human error — such as an employee being duped into making a fraudulent wire transfer — may not be covered.

23%

said their business has purchased cyber insurance to cover email fraud risks

[5] Proofpoint. "Email Fraud Threat Report: Year in Review." February 2018.

CONCLUSION: ON THE RIGHT PATH, BUT MANY STEPS TO GO

Businesses are much more aware of email fraud than they used to be.

In some countries, public sector and government agencies are leading the way by recommending, and in some cases mandating, basic email authentication[6] to protect businesses and citizens.

This push made by government bodies is helping nearly half of those in our survey (47%) to get the budget they need to deploy an email fraud protection solution. In fact, the three countries with the highest levels of email fraud protection — the U.S., the U.K. and Australia — are those whose governments have pushed businesses most strongly to deploy such safeguards.

Yet far too many businesses lack an email fraud defence of any kind.
The main obstacles for those surveyed include:

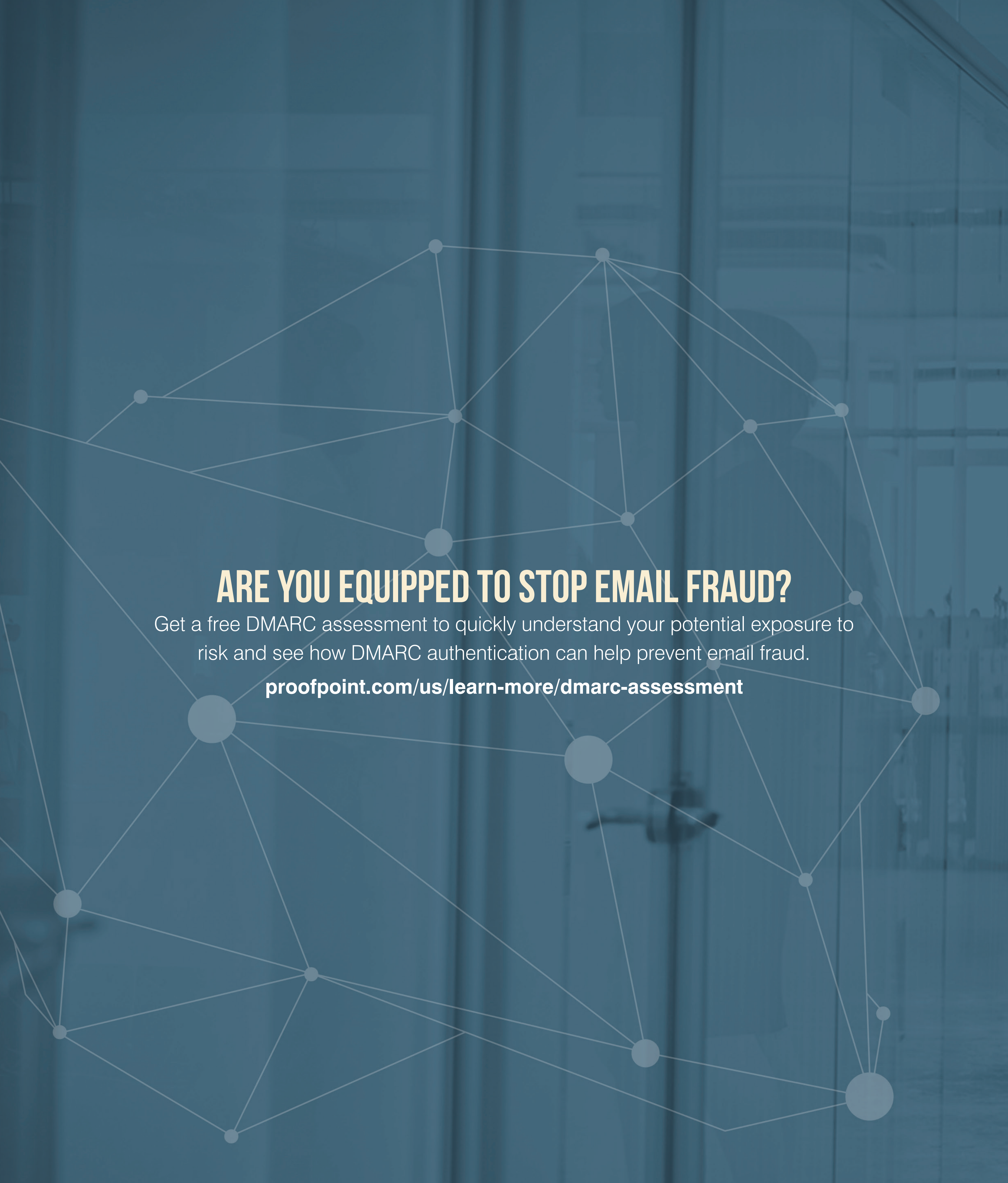
41%	36%	32%	32%	30%
Lack of technical understanding	Lack of budget	Technical complexity of the company's email ecosystem	Lack of knowledge of the issue	Lack of executive sponsorship for the project

Despite large investments in cybersecurity as a whole, the number of email fraud cases continues to rise. Cybercriminals are becoming more advanced. Their tactics are always shifting. And they're growing more effective at evading traditional security tools.

To protect their business, employees, customers and partners, organisations need a multi-layered defense strategy. It should include employee training, financial controls, and especially technology.

For more information on email fraud and how you can protect yourself, visit www.proofpoint.com/uk/emailfraud.

[6] Proofpoint Blog. "U.S. Government's DMARC Mandate: A Step in the Right Direction". October 2017.



ARE YOU EQUIPPED TO STOP EMAIL FRAUD?

Get a free DMARC assessment to quickly understand your potential exposure to risk and see how DMARC authentication can help prevent email fraud.

proofpoint.com/us/learn-more/dmarc-assessment

proofpoint.

www.proofpoint.com