KnowBe4

Could Cyberattacks ‘Turn the Lights Off’ in Europe?

The transition to renewables and geopolitical threats may be leaving the region unprepared for attack

Reliable energy isn't just a convenience – it's the lifeblood of a nation's economy and daily life. From powering homes to driving industries, every transaction, innovation, and manufactured product depends on it. This has long made the energy sector a tantalising target for cyberattacks. In Europe and the United Kingdom (UK), the widespread shift to renewable energy is amplifying this challenge. Adding cyber threats from geopolitical adversaries creates a potential perfect storm, putting regional power stability at risk.

Understanding the Landscape: Renewables, Geopolitics and Recent Attacks

The transformation of Europe and the UK's energy sector has given rise to important advances in wind and solar power, new digitally-native technologies, and new business models, including smart metering, distributed generation, and more. Older parts of the energy infrastructure in the region have undergone digital transformation to bring the new systems online and integrate them into existing operations.

The transition has already resulted in more efficient operations with reduced emissions. Better managed plants and grids have improved service and reliability to customers, strengthening a vital foundation of economic security in the process. The whole process has allowed countries to reduce their reliance on externally sourced energy, decreasing the dependence on fossil fuels from external nations.

However, the adoption of new technologies to support advances in the sector has also created new vulnerabilities, opening the door for cyberattacks on power grids – especially from adversaries seeking to destabilise and demoralise the region. As the World Economic Forum stated in 2021: "As one of the world's most sophisticated and complex industries makes a multifaceted transition – from analogue to digital, from centralised to distributed and from fossil-based to low-carbon – managing cyber risk and preventing cyber threats are quickly becoming critical to company value chains."

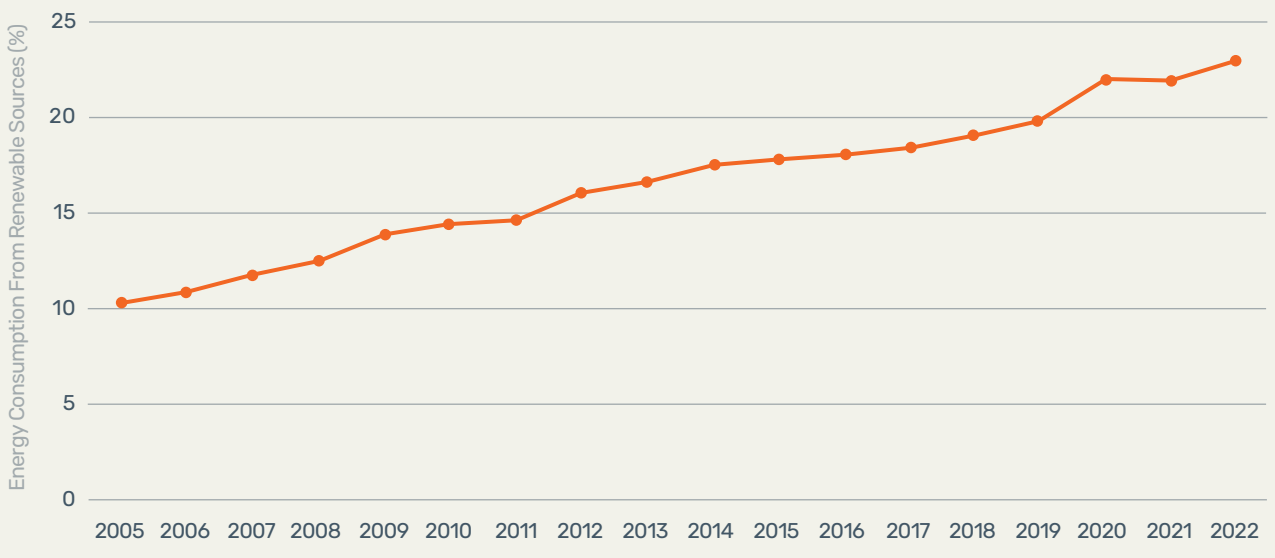
Nation-state Threats

Concerns about increasing cyberattacks on European energy supplies and infrastructure by malicious actors linked to the Putin regime grew following Russia's invasion of Ukraine and the subsequent sanctions imposed by the European Union and the UK.

In March 2022, just one month after the invasion, the European Council on Foreign Relations warned: "The Putin regime, which has long used such disruptive

Share of Energy Consumption From Renewable Sources in the EU

Source: European Environment Agency



tactics, may retaliate against Western economic sanctions with cyber-warfare. European states and energy companies should reflect on the laundry list of such attacks that have occurred in recent years to recognise and respond to the risks they face."[1]

The following month, three wind-energy companies in Germany fell victim to cyberattacks that disabled remote monitoring access to more than 5,800 wind turbines. In one case, the company wasn't even the intended target but suffered "collateral damage" after Russia disrupted Ukraine's ViaSat satellite system.

By November 2023, Politico reported that thousands of cyberattacks had inundated Europe's energy grid since the start of the war. The article quoted Leonard Birnbaum, chief executive of E.ON, one of Europe's largest utilities, who issued a stark warning: "The crooks are becoming better by the day, so we need to become better by the day…I'm worried now and I will be even more worried in the future."[2]

In October 2024, London-based security intelligence firm Dragonfly reported that Russian state-backed hackers had claimed responsibility for a cyberattack on a Lithuanian renewable energy firm in September. The report also detailed attacks earlier in the year, including a breach of a hydroelectric power plant in France in March and multiple ransomware intrusions targeting green energy firms in Germany and Denmark.

Recent Attacks Across Europe

Unlike other sectors, there is little public information available on attacks to the energy sector.

In August 2023, the International Energy Agency in Paris noted that: "Publicly available information on significant cybersecurity incidents is limited due to under-reporting and lack of detection. However, there is increasing evidence that cyberattacks on utilities have been growing rapidly since 2018, reaching alarmingly high levels in 2022 following Russia's invasion of Ukraine."

It noted that globally, the average number of cyberattacks against utilities each week more than doubled between 2020 and 2022, with 1,101 weekly attacks registered in 2022. "Recent cyberattacks in the electricity sector have disabled remote controls for wind farms, disrupted prepaid meters due to unavailable IT systems, and led to recurrent data breaches involving client names, addresses, bank account information and phone numbers. Gas, water and particularly power utilities, are favoured targets for malicious cyber activity." It highlighted that in the EU, companies scrambled to hire cybersecurity experts in the month following Moscow's assault on Kyiv in 2022, indicating that organisations in the utilities sector did not feel fully prepared for unknown cyber threats. [3]

Denmark

In May 2023, according to Danish cybersecurity center SektorCERT, 22 different energy companies in Denmark were breached over a period of just a few days. It was the largest cyberattack in the country's history. The report says the attacks went unnoticed by ordinary Danish citizens but significantly disrupted the operations of the targeted facilities, forcing several to enter so-called 'island mode', where they had to disconnect from the main electric grid and operate independently and autonomously. The threat actor behind the campaign is unknown, but researchers suggest that the attacks were carried out by multiple groups, likely including Russia's state-sponsored Sandworm hackers, who have previously attempted to trigger several power outages in Ukraine.[4]

United Kingdom

According to Chaucer, a UK-based global specialty insurance group, successful cyberattacks on UK utility companies surged to 48 incidents in 2023 from just seven in 2022 – a 586% increase.[5] According to the report, the cyberattacks were primarily data theft or ransomware incidents. As a result, sensitive data from 140,000 individuals was compromised – a 714% increase from the previous year.

A UK-based cybersecurity firm found in a 2024 report that renewables firms in the UK face up to 1,000 attempted cyberattacks each day.[6]

Finland and Sweden

In October 2024, Reuters reported that Finnish utility Fortum is facing cyberattacks "on a daily basis" in Finland and Sweden and has spotted drones and suspicious individuals near its sites, its CEO told Reuters, adding the company had asked the authorities to investigate. Fortum has hydro, wind, solar, nuclear, and combined heat and power (CHP) plants. Security services in Finland and Sweden declined to comment on specific incidents, but both have alleged a pick up in malicious activities by Russia in recent years. Russia has threatened Finland with retaliation for joining NATO and seized Fortum's Russian energy assets worth $1.9 billion last year in response to European Union sanctions.[7]

Germany

On December 4, 2022, German Chancellor Olaf Scholz stated that cybersecurity and infrastructure in Germany are under "severe threat" by foreign adversaries such as Russia and China. He urged the German government to make a "great deal of effort" to arm the nation against such attacks.[8]

The Expanding Threat Landscape: Vulnerabilities in the Supply Chain

Vulnerability in the energy sector isn't limited to just power plants or wind farms themselves – it extends to each part of the interconnected system. Every link in the chain is a potential risk, from transmission lines and distribution networks to supply chain partners, storage facilities, and the vast network of control and communication systems.

"Cyberattacks on Europe's power infrastructure have intensified to the point where energy companies, experts, and politicians were calling for help."

The structure of energy companies, large or small, is complex, normally including different equipment manufacturers, sector partners, and third-party virtual systems that could potentially allow threat actors to endanger the functioning of energy sectors in multiple countries with one attack through one supplier. Conversely, by gaining access to the grid control systems of one company with an outdated system, a malicious actor could cause widespread disruption to entire supply chains and virtual systems.

On a larger scale, the energy sector is becoming increasingly interconnected globally. As this integration occurs, the attack surface grows, with systems and networks spanning across borders becoming more vulnerable.

Even connectivity on the customer level can create vulnerabilities. In solar energy, for example, large-scale solar farms and utility installations are connected to the grid alongside smaller systems like rooftop panels, storage units, and microgrids. As these systems become more integrated, the number of vulnerable points increases significantly. Similarly, at an electric vehicle (EV) charging station, the electrical grid must connect securely to an internet cloud system, which then links to the charging station. The station must also securely connect to the electric vehicle. Each of these connections represents a potential entry point for hackers if cybersecurity measures are not in place at every stage.

This is not to say these points are all wide open. It just means that every time we expand the level of digital services and capabilities in the energy sector, we expand the attack surface.

In the past decade, the European Commission reported that "cyberattacks on Europe's power infrastructure have intensified to the point where energy companies, experts, and politicians were calling for help."[9]

In response, the EU launched the eFORT initiative in August 2024, funding a multi-country research project aimed at addressing vulnerabilities in energy networks. Led by the Spanish technology center CIRCE, the initiative brought together researchers from energy companies and cybersecurity experts from Belgium, Cyprus, Germany, Greece, Italy, the Netherlands, Spain, as well as Norway and Ukraine, to explore ways to improve the reliability and resilience of power grids as Europe transitioned toward a fully digital system.[10]

The eFORT team has been conducting simulations to understand how to protect electric grids from different kinds of cyberattacks. One particular area of concern has been a 'manipulation of demand' attack, where multiple internet-connected energy devices, like charging points for electric vehicles, are tricked into sending misleading information to the power grid.

For example, the grid might receive data indicating a lower demand for electricity than actually exists. The grid would then not be configured to the true demand, leading to potentially widespread outages. By targeting thousands of internet-connected devices, such attacks could trigger large-scale power cuts.

The Challenges

Cost

According to Security Magazine, overall programme upgrades for operational technology (OT) systems and physical infrastructure can cost companies over $100 million; a cost that can be difficult to justify to shareholders.[11] For green companies, meeting the cost can be even further out of reach. For example, wind turbine farms have expansive physical infrastructure but weak physical security. With low short-term returns, safeguarding measures can be viewed as too great a cost even if the long-term benefits are worth it.

Staff resources

IT and security teams in the energy sector tend to be understaffed and under-resourced. OT (operational technology) employees and executives operate without frequent security awareness training and training on modern threats, leaving them open to some of the most common and most preventable attacks. The International Energy Agency (IEA) reports that utilities face significant challenges in recruiting and retaining skilled cybersecurity professionals.

This difficulty is attributed to a global shortage of cybersecurity workers, with an estimated deficit of 3.4 million professionals in 2022. Additionally, salaries offered by power utilities for cybersecurity positions are among the lowest across various industries, further hindering their ability to attract and retain qualified personnel.[12]

Uncertain regulation

Regulatory change is typically slower than innovation. This means there aren't always clear or consistent standards and reporting methods that apply across the different regions and areas that many utilities serve.

Decentralised locations

The decentralised nature of the energy infrastructure means that it is spread across many different locations, such as power plants, substations, and renewable energy installations. This spread makes it harder to secure, as each point in the system could be a potential target for cyberattacks.

Concerns Surrounding the Consequences of Cyberattacks on the Energy Sector in Europe

Growing Global Concern: In December 2024, The Guardian reported that the Swedish government issued a checklist for surviving a war. This checklist not only addressed the risk of "an armed attack against Sweden" but also specifically mentioned the threat of cyberattacks and disinformation campaigns – highlighting the increasing concern about cyber vulnerabilities in the energy sector.

Power Grid Vulnerabilities: In November 2024, British Minister Pat McFadden warned that Russia's cyber capabilities could severely disrupt critical energy infrastructure. "With a cyberattack, Russia can turn off the lights for millions of people," he said, illustrating the devastating impact that cyberattacks could have on power grids and, by extension, the daily lives of citizens.

Regional Energy Disruptions: The threat of energy disruptions caused by cyberattacks is a concern shared across Europe. In February 2025, the Swedish government reissued its pamphlet on surviving crises, with particular attention given to power outages resulting from cyberattacks. The Norwegian government's "emergency preparedness" guide and similar warnings from Finland and Denmark further underscore the increasing focus on preparing for potential energy sector disruptions.

Necessity of Preparedness: Ciaran Martin, former head of the UK's National Cyber Security Centre, emphasised the importance of having a response plan in place for cyberattacks on energy infrastructure. "The difference between being 50% functional within 24 hours of an attack and being offline for a fortnight is huge," he noted, stressing that the impact of prolonged energy disruptions could be catastrophic for both public safety and economic stability.

The Energy Sector and Phishing

Phishing has become the "new normal" for the energy sector, warned Cem Gocgoren, Information Security Chief at Sweden's Svenska Kraftnät.[13] While a threat across industries, its impact here is especially severe. As one of the most common attack vectors, phishing enables cybercriminals to infiltrate organisational systems, often needing only a single compromised account to gain access and move laterally across networks.

The critical nature of the energy sector's infrastructure makes it a prime target for cyberattacks. In 2023, the energy sector reported three times more operational technology (OT) and industrial control system (ICS) cybersecurity incidents than any other industry, with phishing driving 34% of attacks.[14] The complexity of energy networks, combined with the reliance on legacy systems, often leaves vulnerabilities that attackers can exploit.

The fallout isn't just data loss – disruptions to energy supply chains, grid operations, and even public safety can result from successful phishing campaigns. Recent research from August 2024 highlights organisations within the energy sector are increasingly reporting losses in revenue and operational disruptions due to the dual threat of ransomware and phishing, which is driving 94% of energy companies to adopt AI-driven cybersecurity tools.[15] The interconnection between phishing and ransomware amplifies the risk, as phishing often serves as the entry point for ransomware deployments.

Reducing Human Risk for Long-Term Cybersecurity Improvement

Cyber threats against the European Energy sector are continuing, and organisations cannot afford to treat security awareness training as a once-a-year exercise.

Social engineering and phishing remains a primary entry point for cyberattacks, resulting in breaches, ransomware, and destabilised power supply. Frequent training reinforced through monthly phishing assessments can reduce human risk and help users to recognise and respond to threats, decreasing the likelihood of a security incident. Ongoing training leads to fewer clicks on malicious emails and a stronger security posture. To protect critical infrastructure, security awareness must be a continuous effort, not an annual checkbox.

Cyber threats against the European Energy sector are continuing, and organisations cannot afford to treat security awareness training as a once-a-year exercise.

Social engineering and phishing remains a primary entry point for cyberattacks, resulting in breaches, ransomware, and destabilised power supply. Frequent training reinforced through monthly phishing assessments can reduce human risk and help users to recognise and respond to threats, decreasing the likelihood of a security incident. Ongoing training leads to fewer clicks on malicious emails and a stronger security posture. To protect critical infrastructure, security awareness must be a continuous effort, not an annual checkbox.

KnowBe4 Human Risk Management Platform

Each year, KnowBe4 conducts initial phishing security tests within organisations that have not conducted any security awareness training from our platform. The tests are conducted without prior alerts, on individuals performing their routine work tasks without any specialised training. These tests result in a baseline "Phish-prone Percentage," or PPP, that shows the percentage of employees that are prone to click on a phishing link. This is further broken down and applied to specific industries and geographic regions.

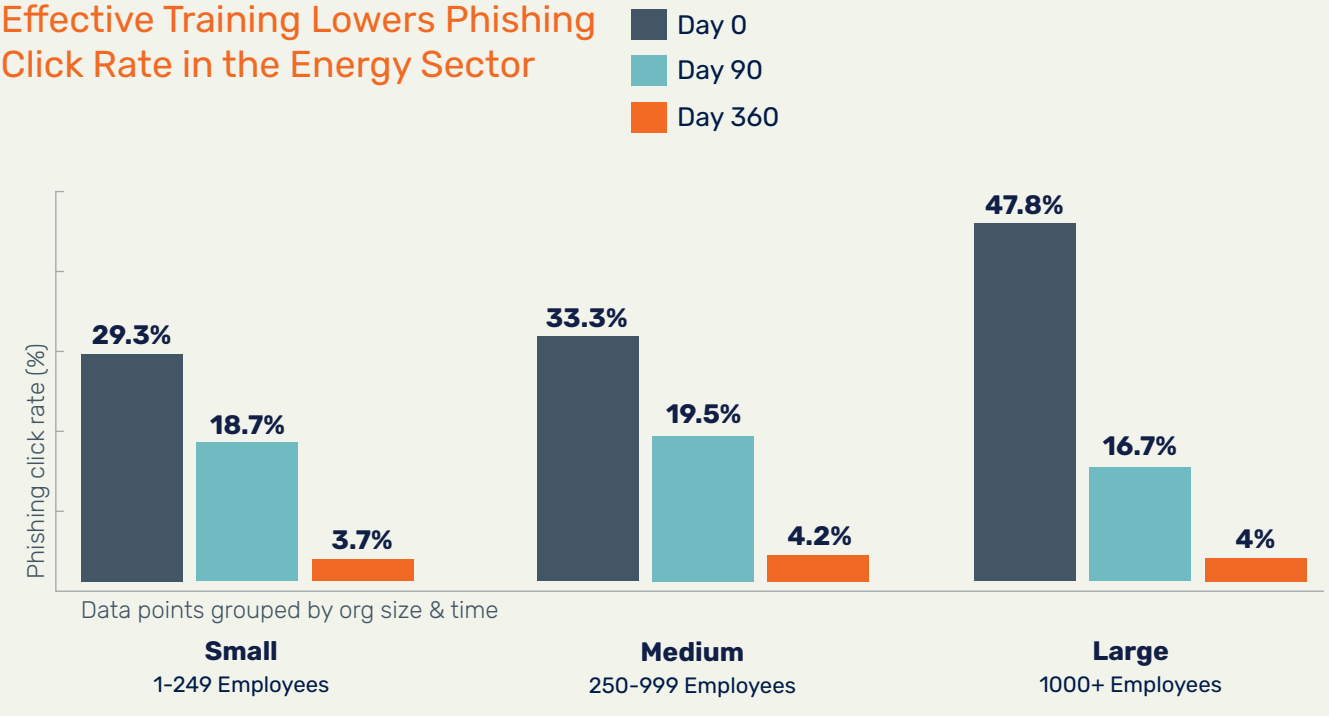
Spanning all industries and organisational sizes, the 2024 KnowBe4 Phishing by Industry Benchmarking Report found that the average PPP stood at 34.3%.[16]

In the Energy and Utilities sector specifically, the baseline PPP for small companies with 1-249 employees was 29.3%. In other words, roughly one out of three employees were likely to click on a phishing link. For institutions with 250-999 employees, it was slightly worse, at 33.3%. As the report notes, one of the most troubling results was found in the "large" Energy and Utilities companies: 47.8% of those tested, almost half, were likely to click on a phishing email.

After 90 days of an integrated approach of educational content along with simulated phishing tests, the picture changed, with PPPs for the Energy and Utilities sector reduced to 18.7%, 19.5%, and 16.7% respectively.

After one year, the findings reinforce the impact of a steady, well-developed security awareness training programme. In Energy and Utilities, the average PPP for small institutions with sustained training dropped dramatically, to 3.7%. For medium sized companies the average PPP after one year had dropped from an initial 33.3% to just 4.2%, while large companies now dropped from an initial 47.8% to just 4%.

Effective Training Lowers Phishing Click Rate in the Energy Sector



Endnotes

1 "Why Europe's energy industry is vulnerable to cyber-attacks," European Council on Foreign Relations, March 7, 2022, https://ecfr.eu/article/why-europes-energy-industry-is-vulnerable-to-cyber-attacks/

2 "Energy grid under cyberattack deluge, industry warns," Politico, https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/.

3 "Current cyberattack trends pose an unprecedented threat to critical infrastructure, such as electricity systems," Casanovas, Marc, International Energy Agency, August 1, 2023, https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind#

4 Antoniuk, Daryna, "Nearly two dozen Danish energy companies hacked through firewall bug in May," The Record, November 14, 2023, https://therecord.media/danish-energy-companies-hacked-firewall-bug

5 "48 Cyber Breaches of Utility Companies Recorded Last Year, a 586% Increase on 2022," Chaucer Group, https://www.chaucergroup.com/news/48-cyber-breaches-of-utility-companies-recorded-last-year-a-586-increase-on-2022.

6 "Europe | Evolving cyber threats to energy sector," Dragonfly Intelligence, October 18, 2024, https://dragonflyintelligence.com/news/europe-evolving-cyber-threats-to-energy-sector/

7 Kauranen, Anne, and Lehto, Essi, "Finnish utility Fortum reports pick up in cyberattacks and surveillance," Reuters, October 11, 2024, https://www.reuters.com/business/energy/finnish-utility-fortums-power-assets-targeted-with-surveillance-cyber-attacks-2024-10-10/

8 Nostlinger, Nette, "Germany's cybersecurity and infrastructure under attack by Russia, chancellor says," Politico, December 2024, https://www.politico.eu/article/olaf-scholz-germany-cyber-security-infrastructure-under-severe-threat-russia-china/

9 "Why Europe's energy industry is vulnerable to cyber-attacks," European Council on Foreign Relations, https://ecfr.eu/article/why-europes-energy-industry-is-vulnerable-to-cyber-attacks/.

10 Allen, Michael, "Guardians of the grid – protecting Europe's electricity supply from cyberattacks," European Commission, October 3, 2024, https://projects.research-and-innovation.ec.europa.eu/en/horizon-magazine/guardians-grid-protecting-europes-electricity-supply-cyber-attacks

11 "Energy sector faces 39% of critical infrastructure attacks," Security Staff, Security Magazine, September 19, 2023, https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks

12 "Cybersecurity: Is the power system lagging behind?" International Energy Agency, https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind.

13 Cyberattacks on renewables and Europe's power sector," Reuters, June 15, 2023, https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/.

14 "Anatomy of 100+ Cybersecurity Incidents in Industrial Operations," Cyentia Institute, https://www.rockwellautomation.com/en-us/campaigns/cyentiareport.html

15 "Escalating Ransomware and Phishing Threats Demand Reinforced Cyber Defences for Energy," Bridewell, August 2024, https://www.bridewell.com/insights/news/detail/escalating-ransomware-and-phishing-threats-demand-reinforced-cyber-defences-for-energy.

16 "2024 Phishing By Industry Benchmarking Report," KnowBe4, https://www.knowbe4.com/resources/whitepaper/phishing-by-industry-benchmarking-report

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk. For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com