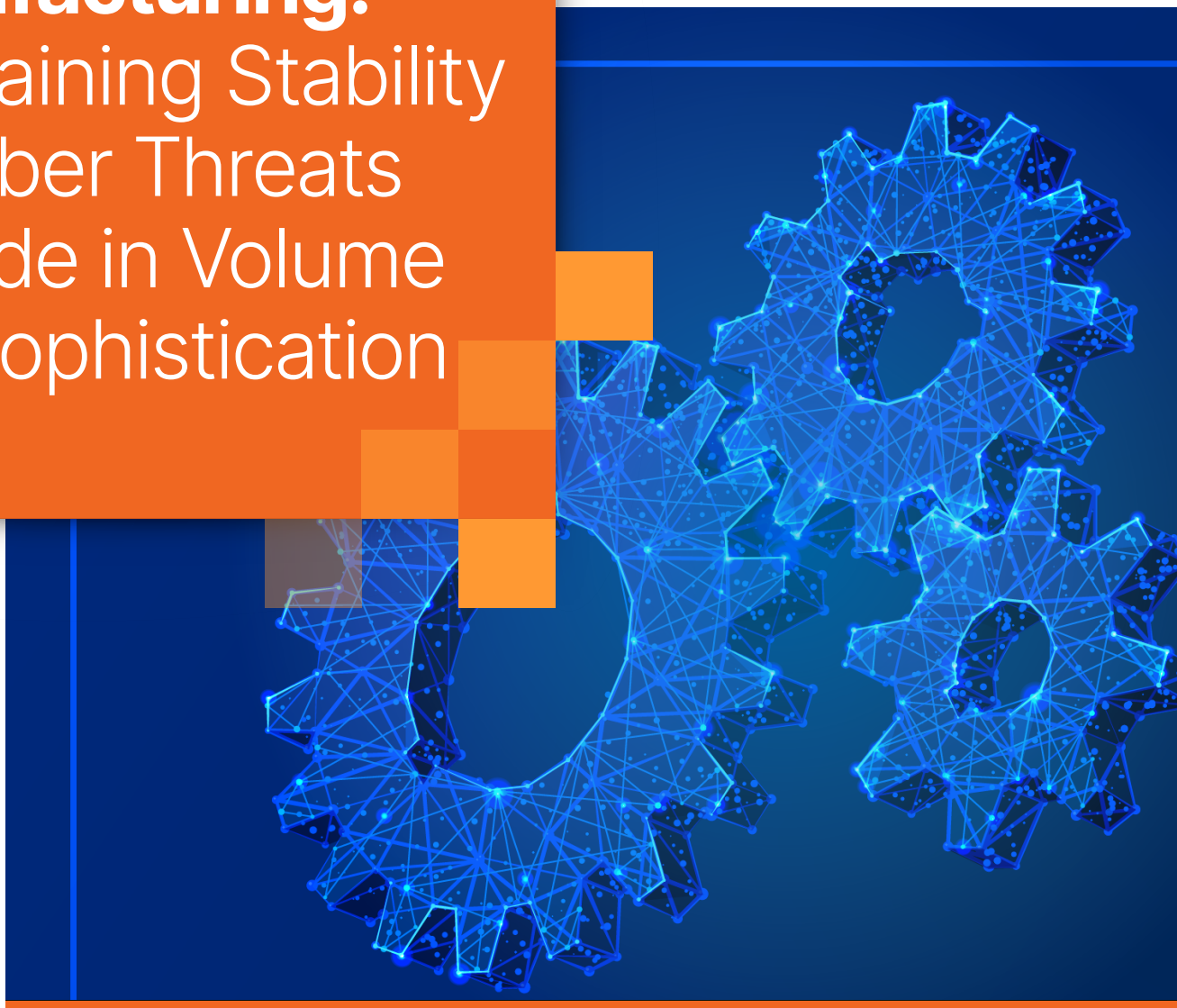
KnowBe4

Manufacturing: Maintaining Stability as Cyber Threats Explode in Volume and Sophistication



MANUFACTURING

Maintaining Stability as Cyber Threats Explode in Volume and Sophistication

The raw materials, processes, equipment, and labor that make up manufacturing are fundamental to commerce, and the foundation of a nation's economic health. The manufacturing sector is also the most frequently attacked by cybercriminals, making security and prevention of attacks a key priority for ensuring the continued delivery of goods and services.

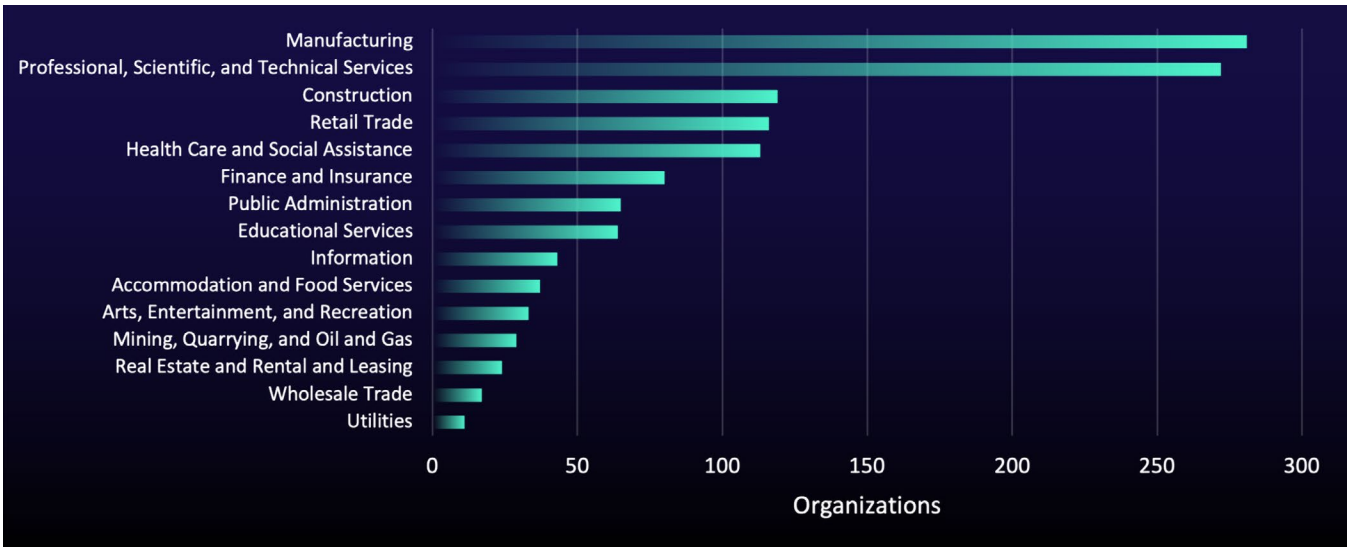
For the third year in a row, IBM's 2024 X-Force Threat Intelligence Report[1] has named the manufacturing industry the most affected by cyber attacks, accounting for 25.7% of all incidents across the top 10 industries. Malware attacks accounted for 45% of those incidents.

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

The X-force findings were echoed in a July 2024 report by ReliaQuest, which also notes the potential high impact of attacks, and the interdependence of IT and operational technology (OT), as contributing to both high ransom demands and a high likelihood of payment, increasing the sector's attractiveness to threat actors.

1 IBM X-Force Threat Intelligence Index 2024, site



Some of the 2023 statistics in the report should be setting off alarms:

- **24%** increase in attacks to industrial goods and services organizations
- **195%** increase in attacks to aerospace organizations
- **92%** increase in attacks against chemicals organizations
- **53%** increase in attacks to automobiles and parts organizations

While the sheer numbers are on the rise, so is the amount of money being paid to the cybercriminals. In June 2024, a Vanson Bourne survey[2] of 585 IT and cybersecurity leaders at manufacturing organizations in the Americas, Europe, the Middle East, Africa and the Asia-Pacific region found that ransomware attacks and extortion payments hit a five-year high in manufacturing and production organizations last year. The average ransom payment in the manufacturing sector, it found, increased 88% to almost $2.4 million in the last year.

There are several factors contributing to the increasing attractiveness of manufacturing as a target:

Interconnectedness of the sector. Whether it is for raw materials, machinery, electrical equipment, digital components, chemicals, or the cars, trucks, ships, and aircraft that transport goods to market, someone up the line is relying on products in the chain to produce and deliver their own goods. The shutdown of production lines in one part of a supply chain can lead to shortages that can potentially cascade around the globe.

Low tolerance for down time. Among other issues, an inability to produce goods resulting from a cyber attack creates product shortages that can result in customers switching suppliers, and encourages the flooding of markets with counterfeit components, starving manufacturers of revenue in both the short and long term. This is all in addition to recovery and forensic costs.

High-value data. Illicitly obtained trade secrets are attractive. In the highly competitive world of manufacturing, getting the intellectual property of competitors can save adversaries millions of dollars, if not billions, in product development research, and shrink time to market timelines considerably.

---

2 Kapko, Matt, “Ransomware attacks hit manufacturing hard in 2023," Cybersecurity Dive, June 14, 2024, site

Global Perspective

Consistent with previous years, the IBM X-force report found that the Asia-Pacific region was the most frequently attacked, accounting for 54% of reported cyber attacks. Europe saw the second most at 26%, followed by North America at 12% and Latin America at 5%.

Some examples of the costliest attacks in recent years:

Europe

On August 10, 2024, Luxembourg-based chemical manufacturing company Orion revealed it lost $60m in a business email compromise (BEC) scam. The firm said a non-executive employee was tricked into transferring the funds to third-party accounts.

In April 2024, a German auto manufacturer reported that hackers had breached the company's systems, stealing sensitive information over several years, including details about gasoline engines, transmission development, fuel cells, and electric vehicle initiatives. At least 19,000 documents related to the company's research and development were exfiltrated.

In April 2024, Dutch semiconductor manufacturer Nexperia was breached by ransomware group Dunghill Leak. In their ransom demand, they threatened to release, amongst other information, design, product, engineering, commercial and marketing data, as well as confidential personnel and client files. Clients named included SpaceX, IBM, Apple, and Huawei.[3]

On March 7, 2024, Belgian brewery Duvel Moortgat detected intruders in their systems, immediately shutting them down, which included halting the production line. Ransomware group Stormous claimed the attack, alleging that they stole 88 gigabytes of data from the brewer.

Asia

In March 2024, Japanese manufacturer of optical products Hoya Corporation was breached by a ransomware group named Hunters International. The group claimed to have stolen 1.7 million files. Production and sales activities were halted as a result of the attack, and labs around the world were unable to process orders for some time.[4]

In November 2023, Chinese automotive parts developer and manufacturer Yanfeng, with global operations in North America, halted production in North America when its computer systems were breached. Ransomware group Qlin later published files including financial documents, non-disclosure agreements, quotation files, technical data sheets, and internal reports to prove they gained access. Several months later, Stellantis, manufacturer of Ram and Jeep vehicles, put in a claim for $26 million to Yanfeng, claiming it was forced to temporarily shut down production due to lack of supply.[5]

---

3 Toulas, Bill, "Chipmaker Nexperia confirms breach after ransomware gang leaks data," Bleeping Computer, April 15, 2024, site

4 Toulas, Bill, "Optics giant Hoya hit with $10 million ransomware demand," Bleeping Computer, April 11, 2024, site

5 Bell, Sebastian, "Stellantis Demands $26M In Damages From Chinese Supplier Sparking Lawsuit," Car Scoops, April 18, 2024, site

Oceania

In August 2024, a large mining company in Australia said it "became aware of a cyber attack." The gold miner said that the security breach had been contained and did not provide further details.

A Japanese car manufacturer reported in March 2024 that the personal information of about 100,000 individuals in Australia and New Zealand was exposed during a cyber attack. The company said an unknown threat actor gained access to the company's local IT servers.

North America

In August 2023, Clorox, manufacturer and marketer of consumer and professional products headquartered in Oakland, California, United States, was infiltrated by a hacker who deployed ransomware to encrypt files and demand ransom. Although production systems were not directly hit by ransomware, processing the order pipeline became challenging without operational supporting systems. Recovery costs exceeded $50 million.[6]

Illinois-based Brunswick Corporation is a billion-dollar boating manufacturing firm operating in 24 countries. In June 2023, a cyber attack disrupted the company's systems, delaying operations in several areas. It took the company nine days to restore all systems. The estimated cost of the attack was $85 million.

California-based Applied Materials is a multi-billion-dollar organization supplying technology for semiconductors. In February 2023, it suffered a ransomware attack from one of its own suppliers. The estimated cost of the attack was $250 million.[7]

In October 2023, a California-based manufacturer of building materials was hit with a cyber attack that caused them to take systems offline, disrupting business operations. The systems remained down for months. The disruption caused the public company's stock to decline by 9.4% over a single month.[8]

Today's Landscape: The Bad Actors Are Getting Better

As digital advances and interconnectedness in the sector increase, the attack surface and the sector's vulnerabilities are widening, with attacks on manufacturing becoming more frequent and more costly. According to Check Point Software's Q2 2024 report,[9] measuring the total number of ransomware attacks that involved extortion, manufacturing again had the "top spot" as the most attacked sector; attacks against manufacturers, it noted, increased by a staggering 56% over the previous year.

---

6 Kovacs, Eduard, "Clorox Says Cyberattack Costs Exceed $49 Million," Security Week, February 2, 2024, site

7 Greig, Jonathan, "Semiconductor industry giant says ransomware attack on supplier will cost it $250 million," The Record, February 17, 2023, site

8 Stewart, Ellis, "Simpson Manufacturing Yanks IT Systems Offline After Cyber Attack," EM360, October 12, 2023, site

9 Check Point Team, "Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years," Check Point, July 16, 2024, site

Industry	Percent out of Published Ransomware Attacks	YoY Change in Number of Published Attacks
Manufacturing	29%	+56%
Healthcare	11%	+27%
Retail/Wholesale	9%	-34%
Finance/Banking	7%	-8%
Education/Research	6%	-3%
Software vendor	6%	-57%
Government/Military	6%	+31%
Transportation	6%	+40%
Insurance/Legal	5%	-25%
Communications	5%	+177%
Leisure/Hospitality	3%	+0%
Consultant	2%	-76%
Utilities	2%	+186%
Energy	1%	-25%

[10]

The growing wave of attacks on manufacturers also illustrates the rising scale of adversaries' ability to increase and execute attacks, and develop new means of intrusion. They have been helped by the development and refinement of the ransomware-as-a-service model, which has lowered the barrier to entry for would-be hackers at the lower end; at the same time, attacks have become more sophisticated. This is in large part due to advances in Artificial Intelligence (AI), which promise to expand the ability of threat actors in the coming years.

KnowBe4, Inc. Founder and CEO Stu Sjouwerman notes in Forbes that generative AI "has introduced an alarming escalation of social engineering threats," including the ability to draft increasingly sophisticated phishing emails without the irregular language and typographical errors that normally serve as red flags to users, and improved voice cloning making it possible, for example, to impersonate family members and con victims into transferring money to them on the pretext of a family emergency. With autonomous agents who can generate a systematic sequence of the kind of tasks that AI Large Language Models work on, Sjouwerman says, "threat actors can carry out highly targeted social engineering attacks at an industrial scale."[11]

10 Check Point Team, July 16, 2024

11 Sjouwerman, Stu, "How AI Is Changing Social Engineering Forever," *Forbes Magazine*, May 26,2023, site

How prepared is the manufacturing sector?

In July 2024, *Infosecurity Magazine* reported[12] that more than half of global manufacturers are inviting unnecessary extra cyber risk by failing to properly implement the DMARC email security protocol.

In a survey of over 4,700 domains belonging to some of the world's biggest manufacturers, the report found that three-fifths (61%) of those surveyed had implemented the Domain-based Message Authentication, Reporting and Conformance (DMARC) protocol designed to prevent phishing by flagging and blocking any incoming emails thought to be spoofed.

44% of those using DMARC, however, had the protocol configured to the least secure setting, failing to quarantine or reject emails flagged as spoofs. Only one-fifth had configured their protocols to reject spoofs.

In July 2024, research from MxD (Manufacturing x Digital), the digital manufacturing institute and the National Center for Cybersecurity in Manufacturing, supported by the U.S. Department of Defense, issued a report, Behind the Firewall[13], that reveals an urgent need for the U.S. manufacturing sector to strengthen its cybersecurity posture. The report finds that manufacturers are overestimating their capabilities in the security arena.

The report found that manufacturers are dramatically overestimating their capabilities and preparedness in warding off and dealing with cyber attacks. Surveys conducted by the group revealed that:

- 76% of manufacturers are confident their organization can prevent cyber risks and respond to cyber attacks.
- Only 34% of manufacturers have comprehensive system security plans (SSPs) in place—a fundamental cybersecurity requirement and often required for compliance.
- Just 43% of all manufacturers have a dedicated cybersecurity leader, such as a Chief Information Security Officer (CISO) or Director of Cybersecurity. The disparity is particularly stark when compared by size: 88% of large manufacturers (500+ employees) have such leaders, compared to 35% of small- and medium-sized manufacturers (fewer than 500 employees).
- Encouragingly, 82% of manufacturers are planning to raise cybersecurity spending in the upcoming budget cycle.

---

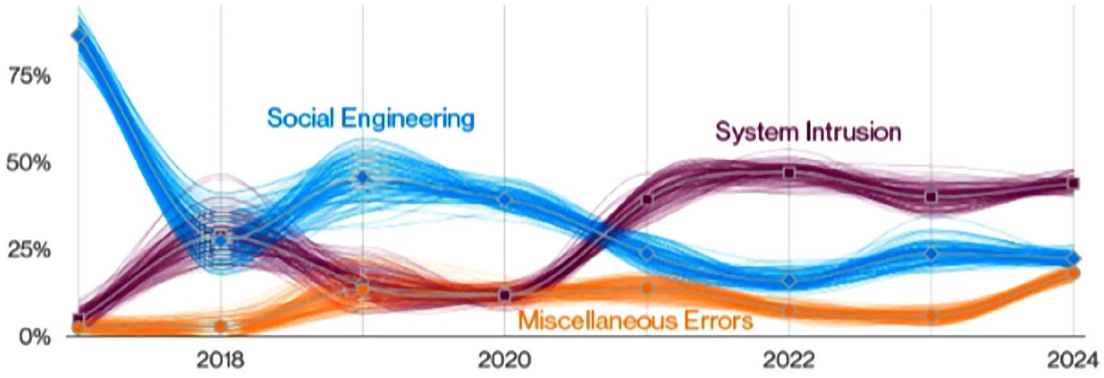
12 Muncaster, Phil, "Just a Fifth of Manufacturers Have Strongest Anti-Phishing Protection," *Infosecurity Magazine*, July 9, 2024 site

13 Assessing Cyber Resilience in U.S. Manufacturing, MxD USA, July, 2024 site

Phishing Their Way In

Unsurprisingly, the IBM Threat Intelligence Report names phishing as the top initial infection vector, followed by exploitation of public-facing applications.

Verizon's Data Breach Investigations Report,[14] which reviewed 2,305 incidents in the manufacturing sector, was even more stark. System intrusion, social engineering (including phishing and pretexting) and miscellaneous errors were the initial vectors in 83% of the incidents. System intrusion has surpassed social engineering for the last four years as the entry point—but it is important to note that in 25% of the breaches, stolen credentials were used to get in. How do you steal credentials? By phishing.



[15]

What They Are Doing When They Get There

The actions of threat actors once they gain access have been shifting in the manufacturing sector. While ransomware still accounts for 17% of the reported incidents,[16] the value of the data they can grab from manufacturers is overtaking the older "encrypt and extort" ransomware tactics.

Manufacturing experienced a 266% rise in information stealing malware being injected into systems — designed to steal logins and other credentials for email, social media and messaging accounts, banking details, etc. Not only do these allow the criminals to return via the stolen credentials; they also command high prices on the dark web. Which explains why credential harvesting accounted for 36% of the most common impacts of manufacturing attacks.

Protecting Vital Production

With the potentially devastating effects of cyber attacks on individual businesses as well as global supply chains, it is becoming increasingly vital to manufacturing companies to have a coordinated strategy for the protection of the sector's operations. Investment in IT staff and well-integrated and updated systems are vital steps to meeting the most basic security requirements. Fortifying technical defenses, including enforcing strong authentication as well as advanced threat detection systems, regularly patching software, and conducting security audits, will help to ensure malicious emails do not get through to the institution's IT infrastructure.

---

14 Verizon Business, "2024 Data Breach Investigations Report" site

15 Verizon, 2024 DBIR

16 IBM X-Force Threat Intelligence Index 2024

But in all sectors, no matter where they end up, nearly all cyber attacks (between 79 and 91%), begin with the cybercriminal gaining access to accounts or servers through phishing or social engineering. The last line of defense—and perhaps the most vital line of defense—will, in the end, be the employee at the keyboard.

Security awareness training to help staff and users recognize and report potential threats such as phishing emails or suspicious activity, including regular training and drills simulating phishing and BEC attacks, not only prevent attackers from gaining access to accounts; they foster a vital culture of cybersecurity that resonates throughout the organization.

Turning Employees Into a Wall of Defense Against Attacks

Each year, KnowBe4 analyzes the online behavior of users to determine a baseline of how many individuals, without security awareness training, are susceptible to clicking on fraudulent links in phishing emails. The initial baseline phishing security test was administered on 11 million users across various industries and sizes, in organizations that had not conducted any security awareness training from the KnowBe4 platform. The tests were conducted without prior alerts, targeting individuals performing their routine work tasks without any specialized training. The baseline statistics indicate a **Phish-prone Percentage™** (PPP) 34% of users; in other words, more than one out of three computer users tested were likely to click on a bad link in a phishing email.

Small manufacturing companies fared well against the baseline. With no security training, the Phish-prone Percentage of manufacturing companies with less than 250 employees was 27.9%, well below average. In companies with more than 1,000 employees, the opposite was true—with no security training, 37.5% of employees tested clicked on a bad link in a phishing email.

The good news is that consistent and comprehensive cybersecurity awareness training works. After 90 days of training, the Phish-prone Percentage in manufacturing companies with less than 250 employees dropped to 19.6%. Medium-sized organizations dropped from 31.6% to 19.8%. Large manufacturing organizations had the most dramatic drop, from 37.5% to 17.4%.

Testing after 12 months or more of sustained training and simulated phishing evaluations showed employees significantly fortifying a company's cyber defenses. In both small and medium-sized manufacturing organizations, the Phish-prone Percentage had dropped to 4.1%; large manufacturing organizations were close, having dropped to 4.3%, below the across-industries average of 4.6%.

It is a fact of life that manufacturing is increasingly dependent on IT and OT, just as the world's production of goods is increasingly dependent on global supply chains. Both increase the sector's vulnerability, and its attractiveness to threat actors. Increasing awareness of and training in recognizing and stopping the flow of phishing and social engineering into manufacturing organizations is becoming increasingly critical to maintaining stability in individual companies, the global sector, and the flow of products into homes and businesses across the world.

Additional Resources

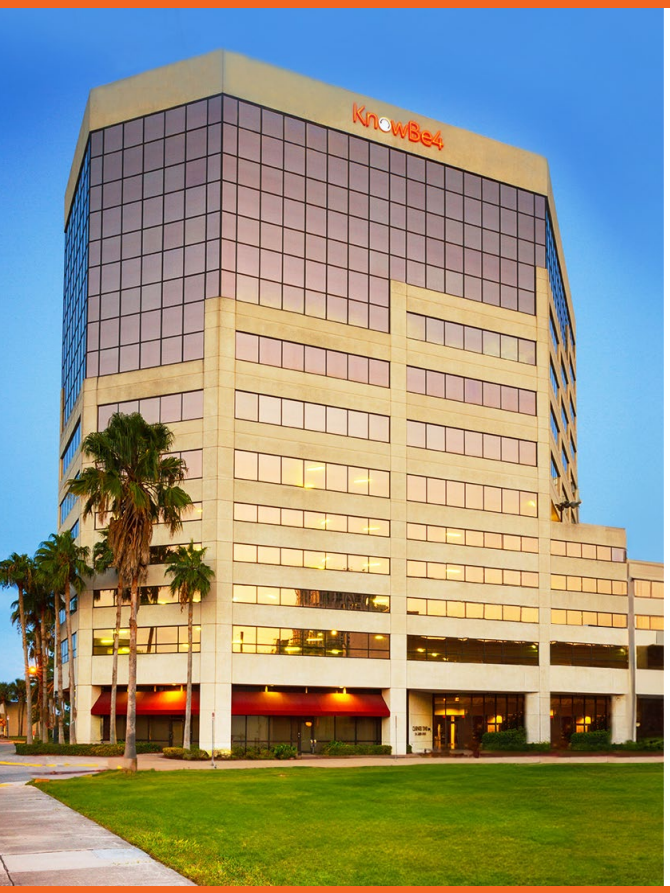
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

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

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 70,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, 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 to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their 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
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E10K01