knowbe4

Human Risk Management For Government

Government organizations of all sizes face escalating cyber threats that can jeopardize sensitive information and disrupt critical services. Human risk management (HRM) is essential to fortify defenses against these threats, empowering employees to recognize and respond to cyber risks effectively. By fostering a culture of cybersecurity, government agencies can significantly reduce the likelihood of breaches caused by human error, social engineering and other vulnerabilities.

Human Error Is The Primary Cause of Government Cyberattacks

~40-50%

of **cyber breaches** within the government sector are caused by human error, according to industry research by IBM, Verizon and Ponemon Institute

$2.1 million

Is the **average cost of a data breach** for the government sector, according to the IBM Cost of a Data Breach Report

204 days

On average, to **identify and contain a data breach** in the government sector, according to the IBM Cost of a Data Breach Report

A Social Engineering Assault

Here are **10 examples** of social engineering attacks that government organizations have suffered in recent years.

1. **A U.S. federal agency** had the personal information of 21 million employees compromised via social engineering tactics.
2. Hackers used spear-phishing emails to gain access to emails and documents of a **U.S. political party.**
3. Fraudsters used social engineering tactics to exploit a **U.S. state economic department**'s unemployment benefits system.
4. Hackers used social engineering techniques to gain access to a **federal law enforcement database,** leaking personal details of around 29,000 employees.
5. **A large metropolitan city** in the southern U.S. suffered a ransomware attack, facilitated by social engineering, that crippled the city's IT systems, demanding a ransom to restore access to the data.
6. A ransomware attack leveraged social engineering to infect a **European transportation department,** causing widespread disruption to operations.
7. An **East Coast U.S. city** was hit by a ransomware attack involving social engineering, which paralyzed many of the city's services and led to a costly recovery process.
8. **A national education department in Asia** suffered a major data breach involving social engineering tactics, compromising 19 years of sensitive personal information and research data.
9. **A U.S. state motor vehicle agency** experienced a data breach where social engineering was used to access employee accounts, leading to unauthorized access to data.
10. **The federal government of a Caribbean country** was scammed out of more than $2.6 million through a phishing attack.

The Impact of Security Awareness Training on Government

Security awareness training (SAT) is the foundation for driving vigilance, building a strong security culture and is the foundation for a HRM strategy.

KnowBe4's Global Phishing By Industry Benchmarking Report measures Phish-prone™ Percentage (PPP), or the number of employees likely to fall for social engineering and phishing scams. Here is the impact that KnowBe4's SAT platform had on government organizations of all sizes based on PPP.

	Small Businesses 1-249 Employees	**Medium Businesses** 250-999 Employees	**Large Businesses** 1000-10,000 Employees	**Enterprises** 10,000+ Employees
Baseline Phishing Security Test Results - No Training	25.1%	26.8%	29.1%	29.9%
After 90 Days of SAT	19.3%	18.6%	17.9%	13.6%
After One Year of SAT	4%	3.7%	4.4%	3.7%
Overall improvement of susceptibility to phishing attacks	**84%**	**86%**	**85%**	**87%**

KnowBe4's HRM+ Platform

The HRM+ platform is KnowBe4's innovative approach to human risk management. HRM+ transforms your largest attack surface — your workforce — into your biggest asset, actively protecting your organization against cybersecurity threats, strengthening your security culture and reducing human risk. It comprises:

Security Awareness Training

AI-powered security awareness training and simulated phishing that allows organizations to drive awareness and change user behavior. Build a stronger security culture by effectively managing the ongoing problem of social engineering.

Cloud Email Security

The only email security platform to continually assess human risk and dynamically adapt security controls, preparing customers to defend against advanced phishing threats, human error and data exfiltration.

Anti-Phishing

Security orchestration and proactive anti-phishing protection to allow your incident response and security orchestration teams to identify and stop phishing threats before they reach your users' inboxes.

Real-Time Security Coaching

The first ever real-time security coaching product that detects and responds to risky end user behavior to provide immediate feedback, improving overall security culture and reducing human risk.

Compliance Plus

Compliance training that delivers continuously updated, engaging, customizable content to users and allows your organization to take a comprehensive approach to security awareness and compliance training.

AI Defense Agents

AIDA is an advanced suite of AI-powered agents that elevates your human risk management strategy.

Learn More About HRM+

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

0449A1025