Case Study

Securing the Human Element

How VanishID Slashed Digital Risk for a Major Energy & Utilities Company

VanishID.

Executive Summary

A leading energy & utilities company with approximately 5,000 employees partnered with VanishID to address a critical cybersecurity vulnerability: the massive exposure of personal identifiable information (PII) of their executives and employees.

This exposed personal data was fueling social engineering attacks, online harassment, and physical threats against executives and their families, after a series of extended outages impacted service operations.

Within just three months, VanishID removed over 1.5 million pieces of exposed PII, reduced executive digital risk by 45%, and decreased the accessibility of sensitive information by 58%. This dramatic reduction in the company's human attack surface has significantly strengthened their overall security posture against data-driven threats.

Firmographics

- **Industry**: Energy & Utilities
- **Size**: 5,000+
- **Executives Enrolled**: 58
- **Employees Enrolled**: 2,598

Digital Risk Exposure

- **Executives**:
  - More than 75,000 exposed PII
  - More than 2,100 data breaches
- **Employees**:
  - More than 1.42M exposed PII
  - More than 36,000 data breaches

The Challenge: A Visible Digital Footprint

As a prominent player in the critical energy infrastructure sector, the company faced unique security challenges. Their executives and key employees, who have access to sensitive operations and information, were particularly vulnerable due to their extensive digital footprints.

Initial scans revealed alarming exposure levels:

- The executive team had over 75,000 pieces of personal information exposed online
- The broader employee base had a staggering 1.42 million pieces of PII available on data broker sites
- Company executives were involved in over 2,100 data breaches containing 135 unique exposed cleartext credentials
- Employees were implicated in more than 36,000 data breaches, containing 2,908 unique exposed cleartext credentials

This extensive digital exposure created a perfect environment for sophisticated social engineering attacks, with personal data readily available to craft convincing phishing attempts, impersonation scams, and targeted attacks against key decision-makers.

The Solution: Continuous PII Removal

VanishID implemented its automated solution, requiring minimal effort from the energy company's security team. The implementation included:

1. **Enterprise-Wide Protection:** Enrolling 58 executives and 2,598 employees in VanishID's continuous PII removal service
2. **User Reconciliation:** Coordinating with the energy company to update enrolled user lists and establish ongoing provisioning and de-provisioning processes
3. **Executive Family Focus:** Launching a focused effort to increase family member enrollment, recognizing that executives' family members often represent an overlooked vulnerability
4. **Continuous Monitoring and Removal:** Deploying automated scanning and removal technology to identify and eliminate PII from data broker sites continuously

The simplicity of implementation was a key advantage—VanishID required only employee names and work emails to begin the protection process, with initial results appearing within 24-48 hours.

Powerful Results: Measurable Risk Reduction

The impact of VanishID's protection was substantial and measurable:

Executive Protection Outcomes

- 45% reduction in overall digital risk
- 58% decrease in PII accessibility
- 86,300 pieces of PII removed

Removal of numerous exposed profiles, including:

- 2,000+ data broker profiles
- 23,000+ personal addresses
- 12,000+ phone numbers
- 4,500+ dates of birth
- 4,500+ work and personal emails

135 unique exposed cleartext credentials were automatically blocked from reuse

Employee Protection Results

- 33% reduction in overall digital risk
- 39% decrease in PII accessibility
- 1,682,848 pieces of PII removed

Removal of numerous exposed profiles, including:

- 50,000+ data broker profiles
- 573,000+ personal addresses
- 365,000+ phone numbers
- 127,000+ dates of birth
- 134,000+ work and personal emails

2,908 unique exposed cleartext credentials were automatically blocked from reuse.

"The continuous nature of VanishID's protection has been eye-opening," noted the company's CISO. *"We thought our digital security was comprehensive, but we'd completely overlooked how much personal information was available on our executives and staff. This service has become a critical component of our security strategy".*

Initial Digital Risk Scores

Current Digital Risk Scores

Understanding Risk Measurement and Mitigation

In the charts above, every dot is an employee. The X axis shows the target's overall **value**, and the Y axis shows the target's **accessibility.**

Access: The Access score measures how accessible a person appears to threat actors outside your perimeter. Scoring includes overall vitals, biographics, openness, and activity metrics.

Higher Access scores = relatively easier for attackers to research, approach, and communicate with.

Value: The Value score measures how attractive a target appears from an attacker's perspective. Scoring includes overall security, privileges, network, and exposure.

High Value scores = most worthwhile for attackers to target, directly or through impersonation.

Ongoing Protection

Over a three-month period, VanishID continued to identify and remove newly posted information:

- 10,300+ additional PII items removed for executives
- 261,800+ additional PII items removed for employees
- Prevented 117 executive-level security breaches by blocking the reuse of compromised passwords
- Protected enterprise data by blocking 1,720 employees from using known compromised passwords

Beyond Technical Protection: Business Impact

The implementation of VanishID's solution delivered several key business benefits:

1. **Reduced Social Engineering Success Rates:** By removing the personal information that fuels targeted attacks, the company experienced fewer successful social engineering attempts against key decision-makers.
2. **Enhanced Security Posture:** The dramatic reduction in exposed PII strengthened the company's overall defense against human-targeted attacks—often the starting point for more severe security breaches.
3. **Operational Efficiency:** Instead of dedicating internal resources to monitor and remove personal information manually, the automated solution handled this complex task continuously, allowing the security team to focus on other priorities.
4. **Family Protection:** The expanded protection to executive family members closed a significant vulnerability gap, as family members are often targeted as indirect entry points to company systems and information.

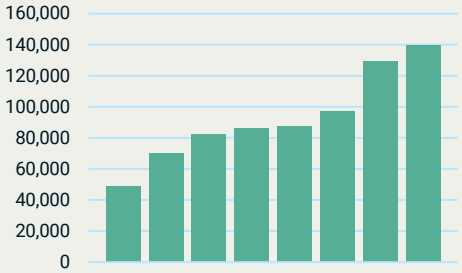
Looking Forward: Building on Success

With the initial implementation showing such strong results, the energy company is now expanding VanishID coverage to include additional family members of high-value targets.

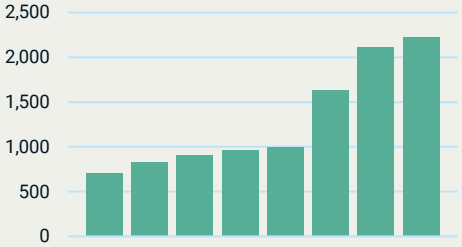
As new executives join the organization, they're automatically enrolled in the protection program as part of the standard onboarding process.

The Energy & Utilities company agreed to share this success story, which has been anonymized for security reasons.

Protected Executives: 58

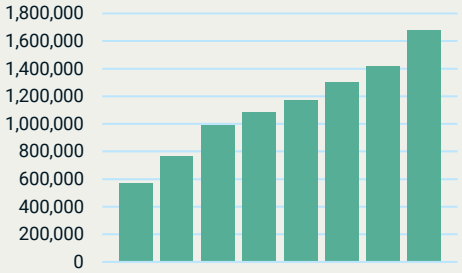


Cumulative PII Removed per Q (Executives)

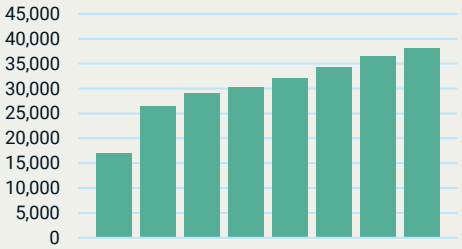


Cumulative Data Breaches Found per Q (Executives)

Protected Employees: 2,598



Cumulative PII Removed per Q (Employees)



Cumulative Data Breaches Found per Q (Employees)

The VanishID Difference

VanishID is the only digital privacy service purpose-built for the Enterprise, providing a turnkey managed service for reducing exposed PII.

By continuously removing personal information from the public domain, VanishID helps organizations prevent harassment and social engineering attacks before they begin, shifting security from detection and response to risk-informed prevention.

Learn more about how you can reduce your organization's target profile with zero effort. Request a demo at vanishid.com/demo.

VanishID

7315 Wisconsin Ave
Suite 400W
Bethesda, MD, 20814

+1 240-316-4067
hello@vanishid.com

VanishID.