INFOSEC IQ™

# Security awareness champions

Success stories from different organizations

# The human element in cybersecurity

Security breaches don't just happen — they often start with a single click, a moment of trust or an honest mistake. According to Verizon's 2025 Data Breach Investigations Report, 60% of breaches stem from the human element.

Small and mid-sized businesses face unique challenges with limited IT resources while still managing valuable data that attracts attackers just like larger organizations. Many rely on IT generalists who juggle multiple responsibilities alongside security.

Security leaders often struggle to implement effective awareness programs with their constrained resources and competing priorities. Many aren't sure where to begin or how to create engaging training that employees will actually retain. Others worry about the time investment required to manage a program or how to measure its effectiveness beyond basic completion metrics.

The organizations featured here overcame these challenges with automation, personalization and data-driven insights. Their experiences offer a roadmap whether you're launching your first program or breaking through a training plateau.

# Reducing employee phishing susceptibility

**Snow College** is a state college located in Ephraim, Utah, facing the challenge of protecting sensitive student data, financial information and personal records.

## CHALLENGE

Snow College needed to protect sensitive data from phishing attacks and build a security culture. Technical defenses weren't enough, as Paul noted: "It only takes one click from a non-aware staff member to circumvent our security infrastructure efforts."

## APPROACH

Snow College deployed Infosec IQ to deliver security awareness training and run phishing simulations for 500 employees while enlisting leadership to endorse security efforts. They used dynamic learner groups to assign targeted training based on phishing simulation performance, focusing additional resources on employees who showed vulnerability to attacks.

## OUTCOME

Snow College cut their phishing rate in half within a year while transforming their security culture. Employees began actively reporting suspicious emails instead of ignoring them, regularly asking Paul to verify potential phishing attempts.

The program demonstrated clear ROI by preventing potential breaches that could damage the college's reputation. Their approach of combining leadership support with personalized training created a sustainable security awareness program integrated into daily operations.

## ORGANIZATION

Snow College

## INDUSTRY

Higher Education

## CUSTOMER

Paul Tew, Information Security Officer

"I get a lot of emails that I never received before the training. People ask me, 'Is this a phish? How do I recognize a phish?' I mean I get literally 10 to 20 a week, which means people are waking up to the risks of their email and how to protect their passwords."

**— Paul Tew**

# Creating a security awareness culture

**St. Catherine's Center for Children**, based in Albany, NY, offers comprehensive human services for Capital Region children and families coping with issues of abuse, neglect, mental illness, homelessness and trauma.

## CHALLENGE

St. Catherine's needed to protect sensitive data for 350 staff and hundreds of vulnerable clients while adapting to remote work. They faced phishing threats and staff turnover requiring efficient onboarding for security awareness.

## APPROACH

St. Catherine's partnered with Infosec to implement new hire and role-based security training for different departments and created specialized modules for short-term staff. They used gamified learning through Infosec's Pick Your Path scenarios and incentivized completion with prizes.

## OUTCOME

The program successfully supported their transition to remote work while maintaining data protection. Staff engagement increased with employees regularly discussing security issues rather than treating it as merely compliance-oriented training.

Employees began applying security lessons in both work and personal lives, creating a holistic security culture. By making security engaging rather than intimidating, St. Catherine's transformed what could have been an IT burden into a valued skill set.

## ORGANIZATION

St. Catherine's Center for Children

## INDUSTRY

Social Services/Non-profit

## CUSTOMER

Mike Urbanski, Director of Information Technology

"Employees tell me all the time they weren't aware of the cyber threats we're teaching them about. It's been amazing to hear how consistent security awareness training has opened their eyes. I'm a big believer that if you teach people in a way that's engaging, it helps them at both work and home."

**— Mike Urbanski**

# Protecting sensitive data with comprehensive training

**HCSC** operates multiple for- and non-profit divisions providing essential services for hospitals, emergency care centers and healthcare providers across Pennsylvania, New Jersey and Maryland.

## CHALLENGE

HCSC discovered an alarming 54% phishing susceptibility rate during testing. With only 11 IT staff supporting 10 locations across three states, they needed an efficient solution while justifying security awareness budget to leadership focused on patient care.

## APPROACH

HCSC implemented automated security awareness training with Active Directory synchronization to streamline user management. They deployed phishing simulations with immediate education for employees who clicked, customizing templates to reflect healthcare scenarios employees would recognize.

## OUTCOME

Within one year of partnering with Infosec, HCSC reduced their phishing rate from 54% to just 10%. Security discussions became commonplace among healthcare staff, with employees actively sharing techniques to avoid phishing during breaks and meetings.

The measurable results generated strong management buy-in and established a sustainable program that didn't burden their limited IT team. This efficiency allowed them to focus on other critical initiatives while maintaining strong human-centered security awareness.

## ORGANIZATION

Hospital Central Services, Inc. & Affiliates (HCSC)

## INDUSTRY

Healthcare Services

## CUSTOMER

David Camardella, Senior IT Director

"Once you set up the product, it's virtually hands off. After every campaign, our phish rate was almost cut in half. I used a lot of the pre-built phishing templates, but I also customized several templates to be more relevant for employees. It has been very effective."

**— David Camardella**

# Increasing security and profit margins

**Fluid Networks** is a California-based managed service provider offering comprehensive business IT, communications and security solutions since the early 1990s.

## CHALLENGE

Fluid Networks needed to protect clients' data across multiple devices and remote access points. They required a security solution that could integrate into their service offering without raising costs while maintaining margins often eroded by time-consuming incident response.

## APPROACH

Fluid Networks shifted from per-device to all-in-seat pricing that included security awareness training. They incorporated Infosec IQ without raising prices, sent biweekly two-minute training modules and added emergency fees for clients who opted out but later experienced preventable incidents.

## OUTCOME

Fluid Networks experienced fewer infected machines, dramatically reducing remediation time and protecting profit margins. This shift from reactive support to proactive prevention improved client satisfaction through reduced downtime while positioning Fluid Networks as a strategic partner.

Their data-driven approach tracked improvements in phishing recognition, helping overcome initial client skepticism about training value. The program transformed how clients viewed security, shifting from purely technical considerations to recognizing the central role of human behavior.

## ORGANIZATION

Fluid Networks

## INDUSTRY

Managed Service Provider (MSP)

## CUSTOMER

Damian Stalls, vCIO Director

"Cleaning up a malware infection can take hours and multiple personnel. Since adding Infosec IQ into our service offering, we've had fewer infected machines, which helps protect our margins."

**— Damian Stalls**

KEY TAKEAWAYS

# How can you lead in security awareness?

Throughout these case studies, successful security leaders revealed several key strategies for building effective security awareness programs:

### Start with leadership buy-in

Get executive endorsement through direct communications and demonstrate the business case by quantifying breach costs. Have leadership communicate security importance to employees and present regular metrics showing program impact to reinforce ongoing support.

### Make training relevant and engaging

Customize content to match your specific threats and culture. Use varied formats to maintain interest and consider gamified approaches. Explore role-based training addressing specific job responsibilities while keeping sessions brief to maximize completion.

### Focus on measurable outcomes

Establish baseline phishing susceptibility rates before launching training. Track improvements in recognition and reporting over time while monitoring suspicious email reports as awareness indicators. Document security incident reductions and associated cost savings.

> “One breach caused by one staff or faculty member can cost exponentially more than the small investment required to train up your people.”
>
> **— Paul Tew, Information Security Specialist**

### Automate and integrate

Leverage automation to minimize administrative overhead and use directory synchronization to maintain accurate user lists. Create dynamic learner groups for targeted training and schedule recurring campaigns to maintain awareness without constant manual effort.

### Create a security culture

Recognize security-conscious behavior and encourage dialogue about security throughout your organization. Coach, rather than punish, and make security relevant to both work and personal life.

## Ready to transform your security awareness program?

Book a meeting to learn more about Infosec IQ and discover how you can implement these best practices in your organization.

# Additional security awareness resources


[Educate your employees with Infosec IQ]

[Launch pre-built training programs]

[Browse award-winning training content]


[Free security awareness training resources]

# INFOSEC IQ

Infosec IQ security awareness and training empowers your employees with the knowledge and skills to stay cyber-secure at work and home. With over 2,000 awareness and training resources, you'll have everything you need to prepare employees to detect, report and defeat cybercrime. Every aspect of the platform can be customized to match your organization's culture and personalized to employees' learning styles. With Infosec IQ, you can:

- Personalize employee training with role-based modules and gamified lessons in a variety of themes and styles to engage learners and strengthen your cybersecurity culture.
- Automate learner management, training campaigns and phishing simulations to keep lessons relevant — and save you time.
- Integrate with your LMS, identify provider, endpoint protection and SOC to streamline program management, reporting and attack response.
- Analyze employee risk scores, learning outcomes and your cybersecurity culture to identify weaknesses and anticipate cyber threats.
- Improve your training efforts with actionable data to make secure behaviors second nature for every employee.

**Book a meeting**

# About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. More than 70% of the Fortune 500 have relied on Infosec to develop their security talent, and more than 5 million learners worldwide are more cyber-resilient from Infosec IQ's security awareness training.

Learn more at infosecinstitute.com.