NINJIO

CASE STUDY

INDUSTRY	REGION	COMPANY SIZE
HEALTHCARE	**EAST COAST**	**5,000 EMPLOYEES**

CYBERSECURITY AWARENESS CHALLENGE

The healthcare industry is an irresistible target for hackers. Healthcare systems are notoriously difficult to secure – according to a 2017 report from the Ponemon Institute, just 25 percent of medical device manufacturers are confident that the "security protocols or architecture built inside devices adequately protects clinicians (users) and patients."

More importantly, healthcare providers are responsible for protecting extremely valuable and sensitive data, such as protected health information (PHI) and electronic medical records (EMR).

No matter how secure a healthcare provider's systems are, there's one vulnerability that even the best technology in the world can't address: employee behavior. For example, as one healthcare executive recently explained to NINJIO: "We've identified that our users are our weakest link. There's just no technology out there that will prevent a user from clicking on a phishing email and compromising the system." This is why her organization has been "looking for a company to partner with that offered training videos based upon real-life scenarios that we can use to enhance our cyber education strategy."

> *"Education is one of the key components of security, and NINJIO does a great job translating real-life security scenarios into fun and informative videos. NINJIO offers the right solution for the right price, and its training falls within the user's attention span – their topics are relevant to today's problems and they provide a better balance than any competitor."*

THE SOLUTION

NINJIO AWARE ANIME & CORPORATE HOSTED PRIVATE PROTAL

The organization wanted to find a cybersecurity training partner that meets a specific set of criteria: Affordability; the ability to provide timely and relevant information that keeps pace with rapidly evolving cyber threats; and content that will immediately engage employees, hold their attention, and ultimately change their behavior. NINJIO meets all of these conditions. As the executive explains, NINJIO provides short and memorable videos that "pertain to all aspects of cybersecurity," while the frequency of new videos provides employees with a "constant reinforcement of cybersecurity scenarios."

NINJIO's solution doesn't just apply to healthcare cybersecurity – it applies to cyber threats that affect users personally. And it's not just that "users are able to apply what they learned in the video to their personal life," as the executive puts it. They can also add friends and family members to their NINJIO account free of charge.

SUMMARY

The organization is particularly concerned about four major types of cyberattacks: password compromise, ransomware, malware, and phishing. In fact, one employee even fell for a phishing attempt – the employee communicated with a hacker and provided access credentials which exposed the organization to the threat of infiltration. Thankfully, the situation was addressed before there was an actual breach of sensitive information, but the scare was a reminder of the threat posed by careless employees.
NINJIO gave the customer an opportunity to address this threat head on with a customized cybersecurity training solution that can address particular attack vectors like phishing. For example, the executive points out that her organization realized that the employee who fell for the phishing attempt "needed additional training," and the cybersecurity team could "address the problem directly by sending a NINJIO video related to that type of hack."

Before the healthcare organization started working with NINJIO, the security team had no way of tracking compliance with its cybersecurity initiatives.

NINJIO plugs right into its existing learning management system (LMS), which gives it a much more comprehensive picture of the effectiveness of its cybersecurity platform. Moreover, the organization is confident that compliance will continue to increase.

RESULTS

The rate of compliance is consistently increasing.

The company had no way to track compliance until partnering with NINJIO.