PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

TIM CALLAHAN
CISO, **AFLAC**

HEADQUARTERS: COLUMBUS, GEORGIA

EMPLOYEES: 8,000 EMPLOYEES & 17,000+ INDEPENDENT AGENTS

ANNUAL REVENUE: $23 BILLION

In a business where one misstep can have serious consequences, it is no wonder that Aflac CEO Dan Amos has prioritized as strong a security program as possible. Take a look at Target and Anthem, two recent examples of what can happen if your system is hacked by unscrupulous criminals intent on damaging your brand. One thing has become increasingly clear, and that is that every company falls under two categories: those who have been breached and those who will be.

Aflac, the leading provider of voluntary insurance in the nation, takes its brand seriously. To that end, each and every employee feels like an ambassador of sorts – a protector of the company's hard-earned reputation.

"The employees here really take our brand personally. Everyone wants to protect it. It is among our most valued assets," said Tim Callahan, CISO at Aflac.

Callahan believes that the respect employees have for Aflac's image, one of the most recognizable brands in the United States, is a major contributor to the success of the company's security program.

"Our clients and the brand are inseparable, which has built a lot of synergy for our program," he said.

Our clients and the brand are inseparable, which has built a lot of synergy for our program.

Aflac is consistently ranked by the Ethisphere Institute as one of the World's Most Ethical Companies, a designation that truly matters to the employees. Callahan sees his mission as CISO as doing everything in his power to help prevent a security issue from negatively impacting the company's record for ethics and accountability.

"I know people at Target, and the employees there value that brand as well. They took it personally when the company's data was breached,"

he said. “So when I hold awareness talks, I explain to our employees that as a well-trusted brand, more is expected of us. Client expectations are very high.”

According to Callahan, employee commitment to the brand and client trust are key components of security awareness. When employees see the importance of security in building that trust and protecting policyholders, they are more inclined to demonstrate the faith Aflac needs to provide the best services in the industry. A trusted relationship, built over time by always treating customers and partners with respect, has helped Aflac provide data security. In fact, Callahan says that the company regularly conducts social engineering tests and takes great pride in how well employees perform.

COMMITMENT TO SECURITY STARTS AT THE **VERY TOP**

As with any important initiative, success often hinges on executive buy-in. After a recent briefing about the issue, CEO Dan Amos proposed a security contest for employees as a means to maintain momentum that had been building with regard to ensuring data security. The contest ended with a generous reward for the best cybersecurity recommendations.

“We had some great ideas, including the creation of a Security Ambassador program comprised of volunteers from various departments who take on additional training and act as a liaison between the security team and the business unit,” Callahan said.

The Aflac team performs a number of standard security awareness programs within their “SAFE” program, which stands for “Security Awareness for Everyone” and is represented by a rendition of the famed Aflac Duck with a safety logo and uniform. The program includes lunch and learns, entertaining video clips and one-on-one educational sessions.

“We teach them how to protect themselves at home, and of course, all of those practices are transferrable to the workplace as well.”

Callahan meets regularly with the executives at the highest levels in both the U.S. and Japan. He co-chairs the Global Information Security Council and the U.S. Information Security Oversight Committee (ISOC) for the company. These two groups include senior leadership members such as the deputy general counsel, CIO, head of audits and chief compliance officer. Callahan meets at least monthly with the U.S. ISOC, at which time they review risk and policies.

SECURITY REQUIRES INDUSTRY-WIDE **COLLABORATION**

Callahan spent many years in the financial services industry and was one of the early members of FS-ISAC:

“We share information about preventing attacks, and from there each company is able to act on the intelligence within their own environment. I see retail and health care starting to adopt some of these best practices as well, and it is a good thing.”

In an industry like insurance, where any company can be the target of the actions of criminals it’s hard to argue against keeping data security at the top of everyone’s priority list.

> “We had some great ideas, including the creation of a Security Ambassador program comprised of volunteers from various departments who take on additional training and act as a liaison between the security team and the business unit.”