

CASE STUDY

Revolutionising security awareness at a leading financial services institution



In numbers

86,000
people

10% of Credit Suisse staff **now use longer, stronger passphrases** than they did before

92% of users now consider themselves **more responsible for security than before**

81% have a **more positive attitude towards security**

Average **confidence in cyber security has increased** since deployment

About Credit Suisse Group

Credit Suisse is a leading global wealth manager with strong investment banking capabilities. Headquartered in Zurich, Switzerland, its operation has a global reach and extends to about 50 countries worldwide across mature and emerging markets with more than 45,000 employees from over 150 different nations.

Credit Suisse partners across countries, divisions and regions to deliver holistic financial solutions to its clients, including innovative products and specially tailored advice, aligned to its high ethical standards. It strives for quality and excellence in its work and professional relationships.

Deployed:



Awareness
Hub



Behaviour
Change Hub



Culture
Hub



Challenges

Developing a cyber security culture

When Caroline Bansraj joined Credit Suisse as the Global Training, Awareness & Communications Director some five years ago, the company was already engaged in basic human cyber awareness activities. Phishing exercises, mandatory training, and newsletters were all in place. At that time, these inventions put the company ahead of many of its peers. But Bansraj knew that Credit Suisse could do so much more.

She soon got to work building out a human cyber security programme focusing on the individual: "My strategy was about people - about the 'you'.

I wanted a programme that got through to people that cyber security matters. People need to know why it's important, and they need to know why it's important outside of work as well as inside."

While Bansraj made early progress, to continue to reduce the firm's human cyber risk, she felt she needed to shift her approach. "I was two and a half years into building into a bigger programme, and I was

reaching the point where I was thinking, 'what next?'. 'How can I take this further?'. For me, the answer was about **developing a cyber aware culture.**"

To support the development of that culture, Bansraj knew that she needed to take an innovative approach to cyber security metrics. Credit Suisse had few **data-points with which to gauge whether human cyber inventions were working.** The company had access to some basic phishing metrics and some communications metrics, but this in itself was insufficient for inducing changes to behaviours and attitudes.

"There was **nothing to indicate that what the company was doing was working,**" she notes. "There was nothing tangible. We might have known if people were opening our newsletters, for example, but it was impossible to say whether any of this was having any impact on our culture. And even though we were tracking feedback from staff, there was a feeling that people may not necessarily be honest."

Choosing CybSafe

A platform that does things differently

Throughout her time at Credit Suisse and while building out her new programme, Bansraj was pitched frequently by different vendors. None stood out as being able to support her desire to build a cyber culture - until CybSafe.

"Everybody claims their solution is the best, and that they're going to solve your cyber awareness challenges almost overnight," Bansraj comments. "When CybSafe's CEO, Oz, spoke to me about their offering, it struck me as something genuinely different. It **wasn't just a training and awareness tool.** The platform was so well-rounded and innovative. It was full of elements that took it much, much further than all the others."

Seeing a demonstration of the product cemented that interest. "It was a key point in my decision-making process", she says. "Seeing that CybSafe could be **tailored to people's individual needs** and appetites was a real moment where I knew that the solution was a cut above the rest."

"Why did I pick CybSafe? Ultimately, it was about the people-centric nature of the platform. It **wasn't about ticking a box.** It wasn't saying, 'if your employees do this then you can satisfy regulators and the board.' **Here was a platform that could actually empower people.** And that was a game-changer."

Impact

Empowering and engaging people

CybSafe now fills a central role in Credit Suisse as part of a broad multi-channel alongside emails and intranet messaging.

One of the major changes Bansraj has seen is in terms of the engagement people now have in cyber security. People enjoy using the platform because it's ultimately something that benefits them. "It's not a chore. It appeals to people on a personal level. It helps them. It protects them. And people are grateful for that. CybSafe makes cyber security matter."

The Family and Friends feature is one of her highlights. "**People are more empowered and more knowledgeable.** And they **share that learning with other people** – with colleagues, with friends, with family. This positive ripple effect is one of the big



USPs for me. That you can share content with people outside of the platform is a revelation for people."

CybSafe's security awareness training, certified by the NCSC and CII Sec, has also been a valuable resource for the firm. These short, focused security awareness modules provide people with all the tools and information they need, empowering people to protect themselves, their organisations and their families online.

"The **modules are made for everyone**," Bansraj explains. "It doesn't matter what your level of knowledge is. CybSafe's phishing content is particularly useful, as malware is often hard to explain to people in an easy way. Content around the correct use of wi-fi is fantastic too."

Data and metrics

Quantifying cyber security culture

One area of CybSafe Bansraj is keen to stress is the **value of her data**. Bansraj uses the rich data sets produced by the platform to report to Credit Suisse's Global CISO and even industry regulators. Beyond reporting, data is also at the heart of her continued efforts to develop a better cyber security culture.

Security culture is the invisible glue that links all Credit Suisse's security awareness activities and the thing that makes secure behaviours possible. With Culture-IQ and Sentiment-IQ, Bansraj can now

measure her security culture and knows what she needs to do to make it better.

Cyber security culture assessments help predict **where risky behaviour will occur**. And **anonymous sentiment data help illuminate the causes**. As Bansraj explains, "we have the tangible information we need to learn about our own culture. And we get **honest feedback** about where we can make changes."

Support

Not just a relationship – a partnership

"The level of service my team gets from the CybSafe team has been amazing," Bansraj says. "They are **so responsive and supportive.**"

Further to the timely and reliable support, Bansraj appreciates, most of all, how connected she's become to the CybSafe family: "**We went into this as a partnership. This has never been a client-vendor relationship.**" There is a huge value add from the connection, whether that's being involved in PeepSec,

or involving the CybSafe team in our events here at Credit Suisse. CybSafe is honestly **an extension of our awareness team** and they're always happy to listen to our ideas. It's been remarkable."

Insights from users

"An interesting insight into the realities of security today."

"These tools are absolutely superb!"

"A great initiative and extremely useful."



We are CybSafe. A British cyber security and data analytics company. We make it easy to manage human cyber risk.

Our software gets people engaged in security. It empowers them to make the best everyday-security decisions possible. We use behavioural science, data and reporting metrics to help security professionals do their jobs better. And see their impact on people-related cyber risk.

Our customers report improved security habits and fewer people-related security incidents.

[Try it yourself](#)

