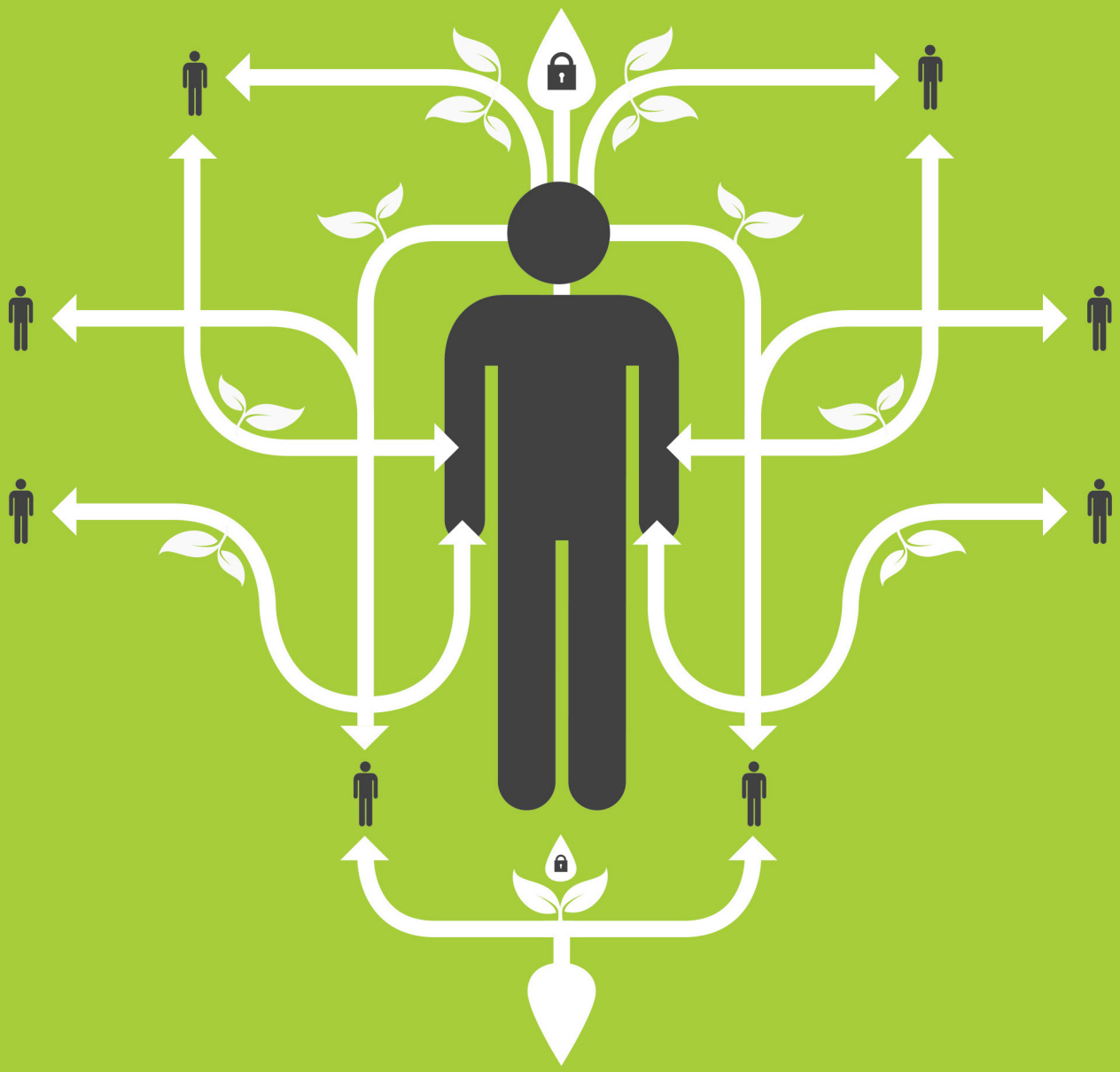


SUREVINE

REALTIME SECURE INFORMATION SHARING

CASE STUDY

THE NEW FRONTLINE IN CYBER DEFENCE

SUREVINE
REALTIME SECURE INFORMATION SHARING

THE NEW FRONTLINE IN CYBER DEFENCE

A wave of hacking incidents are testing organisations, businesses, government and critical national infrastructure on a daily basis. According to a recent report, nine out of ten large organisations have suffered a security breach, meaning it is now a case of when - not if. Businesses must ensure they are managing the risk accordingly, especially when the average cost of a security breach to a large organisation is between £1.46m and £3.14m; a figure that is growing year on year.

In order to combat the cyber threat, the UK is leading the way for organisations to actively share and collaborate on information about new risks and vulnerabilities via a trusted online community. The secure platform, CiSP (Cyber-security Information Sharing Partnership) collaboration environment, now owned by the National Cyber Security Centre (NCSC), acts as an early warning system and was developed by technology startup, Surevine.

WHO ARE SUREVINE?

Surevine builds secure, scalable collaboration environments for the most security conscious organisations who need to share highly sensitive information; joining people up securely and enabling a real-time response to cyber threats and incidents.

The company was founded by Stuart Murdoch and John Atherton, both of whom have an established track record of delivering landmark secure systems, including systems for UK Central Government. Surevine's secure collaboration technology is relied on by thousands of people around the world to securely share and collaborate on sensitive information.

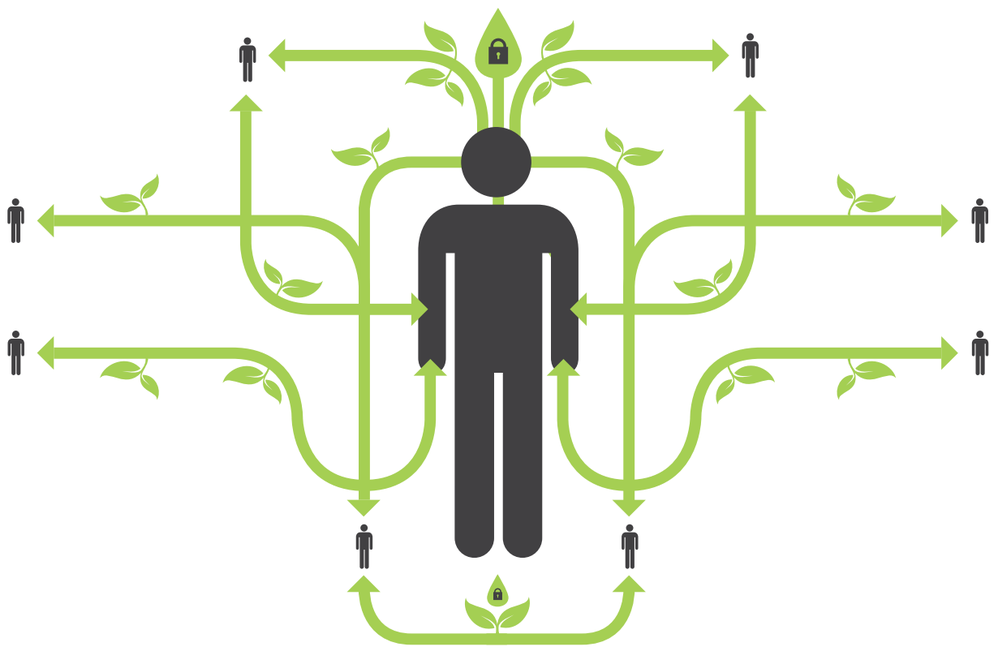
In 2016 Surevine received a high commendation for Technology Excellence at the BCS & Computing UK IT Industry Awards.

THE PROJECT: CYBER-SECURITY INFORMATION SHARING PARTNERSHIP (CISP)

In 2013, responding to the growing threat from both overseas and domestic cyber attacks, Surevine developed a secure collaboration environment for cyber incidents; known as the Cyber-security Information Sharing Partnership (CiSP).

The primary objective of the CiSP was to help organisations improve their Situational Awareness and response to cyber incidents. Members would be able to share and communicate with businesses in the same sector which may be subject to the same type of risks and cyber threats, and gain insight into what was happening across other sectors.

In order to be effective, CiSP needed to provide members with a highly secure collaborative environment in which to share real-time information about cyber threats.

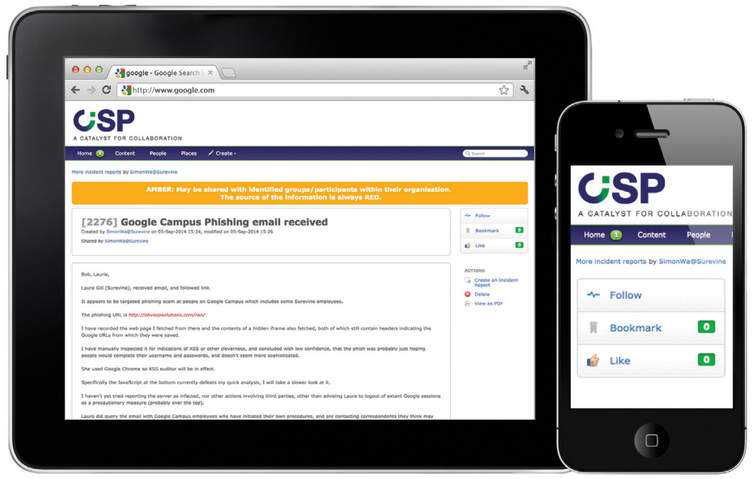


THE SOLUTION: SUREVINE...

The first iteration of CiSP was launched out of a pilot called Project Auburn, which attracted around 80 organisations from across a number of key UK industries. As a known provider of secure collaboration environments, and a trusted partner to UK Government, Surevine was engaged to build the secure online collaboration environment which would form the backbone of CiSP. Although the project's urgency demanded a very challenging deadline, Surevine delivered the environment on time and on budget, alongside project partners Lockheed Martin and BT.

Surevine's CiSP platform had, at its heart, the features of an enterprise social collaboration platform, extended to meet specific needs of cyber-security information sharing, and required rigorous security testing to meet the demands of such national significance.

- Anonymity was added, allowing users to share information without attribution to themselves or their company to allay concerns about reputational damage or liability.
- All content was marked with a "handling" level, ensuring that sensitive information is handled correctly.
- Multi-factor authentication was added, increasing the environment's security.



THE IMPROVEMENT: WHAT HAS SUREVINE ACHIEVED FOR CiSP?

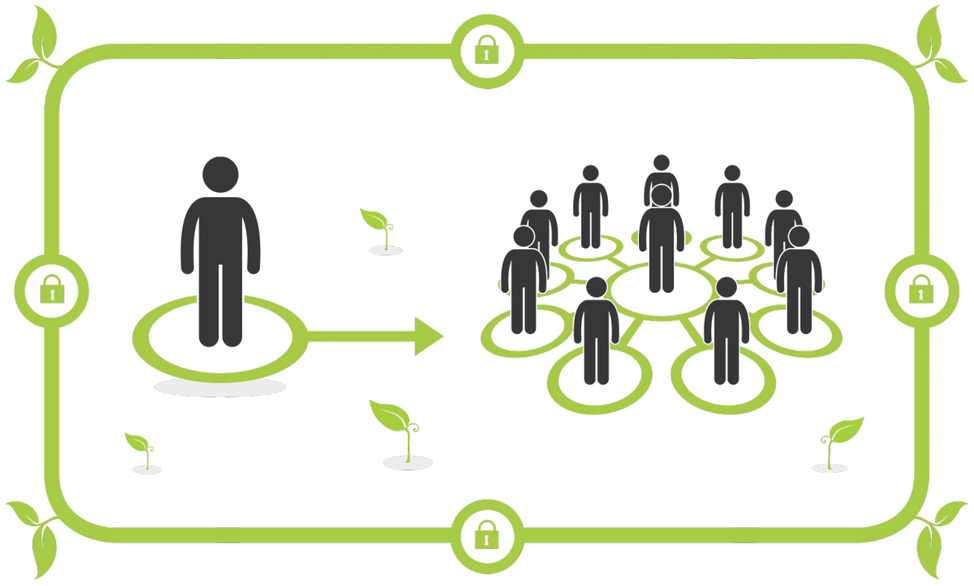
Today, the platform is home to thousands of network defenders - cyber security professionals sharing and collaborating on behalf of their employers, which comprise of critical national infrastructure including financial services, energy, utilities and telecommunications. Alongside these organisations are academia, government and a wide cross-section of industry, including Small to Medium Enterprises (SMEs).

Surevine's project has been more successful than anticipated. According to CERT-UK: "We had a ministerial target of 500 organisations to reach on CiSP by the end of 2014. When the final total was compiled at the end of the year, we had exceeded this target by over 50%, reaching a total of 777 organisations and 2,223 individuals on the platform."

As of December 2017, those figures stood at over 4,000 organisations and over 9,000 individuals. Cyber-security specific features of the platform include a structured cyber incident reporting system, ensuring participants can quickly report or respond to incidents shared in a consistent and concise format. This has reduced the time taken for network defenders to see, ascertain and act on threats.

Surevine also implemented the intuitive Traffic Light Protocol (TLP) approach to information sharing, ensuring participants only pass contributed information within and beyond the network if the colour designated by senders allows it. This has made members more comfortable sharing information for everyone's benefit.

Indeed, the CiSP platform implemented by Surevine is used by the UK government to pass specific security alerts to companies around the country. It also supports anonymity so that, for example, an employee of a particular bank could confidently alert other CiSP member organisations about an ATM system failure following a cyber incident, and provide tips that may help a rival bank avoid the problem, without attribution.



WHY SUREVINE?

Surevine has a solid track record of delivering collaboration solutions to the core of UK central government. Prime Minister David Cameron highlighted Surevine as **one of the UK's leading cyber security companies,** and an early Surevine-developed collaboration platform for joining-up core central government departments was singled out for praise by the last two Prime Ministers.

To date, the company has implemented around 70 collaboration projects for government and other organisations with the most demanding security requirements, supporting tens of thousands of live users.

Considered a trusted partner of government, Surevine's debut project - a social networking collaboration environment for a UK government department - was praised by the then government Chief Information Officer as "the best example of intelligent use of social technology for internal collaboration across the whole of government" and achieved widespread buy-in within just weeks.

The uptake of the debut system was viral, partly because Surevine's people-centric environments aim to make systems intuitive and to actively encourage participation, whilst respecting roles. These boundaries and circles of trust must exist because the information being shared is precious, and the person sharing information must remain compliant with the policies their organisation works within.

TIGHT SECURITY FROM OPEN SYSTEMS?

Surevine's technology, ethos and architecture are open, meaning the beneficial impact spreads far beyond its initial customers. An adherence to open standards allows systems to be interoperable with a wide range of other technologies. For instance, one of Surevine's earlier code bases has been forked by a US federal government agency to deliver a LinkedIn and Twitter-style social networking and collaboration platform with over 35,000 registered users. There, it is helping improve and speed up interactions, remove duplication and reduce reliance on email.

But open technology does not mean an open door. By being open, Surevine technology is open to more scrutiny, allowing for more rigorous testing than a closed system.

WHAT'S NEXT?

Using Surevine's platform, NCSC aims to encourage even more participants across UK organisations, spreading the security benefits to an ever-greater number of organisations and infrastructure providers.

It is part of NCSCs mission to connect with other CERTs around the world to present a united face against the threat. Neither hackers nor internet best practice know national boundaries - so the inclusion of more expert voices will positively impact on reducing risk even further.
Surevine continue to develop, enhance and support the CiSP, including the development of mobile access to improve threat notifications and enhance participation.

KEEPING THE WORLD SAFE

2018 brings the next generation of the system underpinning CiSP, Threatvine, which has already launched across an international market.

Secure communities powered by Threatvine bring together business, government and academia; moving beyond cyber security information sharing to collaborative cyber security intelligence analysis, keeping them one step ahead of the cyber threat.

REALTIME SECURE INFORMATION SHARING

surevine.com • info@surevine.com

UK +44 845 468 1066 • US + 1 202 517 6966

18.01.ncsc