Strategy for Jisc security products and services (2015-2018)

Vision

The vision of this strategy is to help research and education institutions increase their capability to respond to online security concerns and to help them undergo the cultural change required for effective information security. Achieving this vision will help institutions protect themselves and their users and instil confidence within government and industry in the sector's ability to protect assets and individuals from security risks and vulnerabilities online. Within an information management, assurance, governance and network security context we aim to make the UK one of the safest places in the world to perform innovative network-based research and education; and to help the UK research and education sector develop and implement new approaches that reduce the risk from cybercrime.

Mission

Our mission is to safeguard the current and future network and information security of the Janet network and of our customers' networks, creating a secure environment for our customers and their users to conduct innovative online activities. To do this we will continue to develop and refine products and services to help support an institution's information security policy and to ensure continuity of business.

Context

Recent events have served to focus media attention on cyber security, but this has long been an area of activity for those responsible for providing, protecting and supporting services in research and education. Research and education networks developed the first Computer Emergency Response Teams in the 1990s and are still recognised as leaders in incident response, however the environment that we work in is changing. Whereas most incidents used to be reported in the form of an emailed complaint sent by a human, we now receive the majority of information from automated systems run by third parties. We also receive considerably more information now, with more than ten times as many incidents reported compared to 8 years ago and a typical 24 hour period can see around 900 items of security intelligence being received concerning more than 200 separate customers.

In 2010 the UK Government rated cyber attacks as a 'Tier 1' threat and subsequently in November 2011 published the UK Cyber Security Strategy[1] with an increasing emphasis on protecting UK digital infrastructure. Advanced e-infrastructure has always been essential to the success of UK research and education, however, it is exposed to an environment with increasing potential to disrupt or damage it. Modern security risks normally target weaknesses in human, organisational and technical security; an effective response to these cannot be limited to IT alone but must involve the whole organisation.

Strategy

This strategy focuses on the Jisc services and products that can help organisations address the technical aspects of cyber security (protecting systems, networks and information) and also aims to change the attitudes and behaviours of organisations and users of their networks.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Customer and user requirements

To continue providing a world class service we will seek to enhance the customer and user experience through understanding their challenges and needs for online security, and implementing robust services to respond to these needs no matter how large or small their organisation. Current challenges and requirements identified by institutions as areas we can help are:

- Help in providing advice and guidance for information security;
- Help in maintaining system and network uptime;
- Confidentiality of information during processing, at rest, and in transit;
- The means of ensuring the integrity of information is protected;
- Ensuring availability of information by those authorised to access it;
- Help to identify, assess and manage information security risks;
- Help in determining whether an institution's security measures are proportionate to risk.

Strategic responses

To deal with the changing landscape we will increase our coordination role nationally and internationally – particularly with regards to multi-agency coordination, bringing organisations and people together to best protect our community. Working with partners and colleagues across the sector we will help coordinate activity in working towards a common goal of minimising the possibility or effect of cyber attacks.

We will continue to actively work with national and international partners, including with law enforcement bodies, on incident response and prevention, including the international CERT community, to ensure we are aware of both technical vulnerabilities and information about specific hosts on Janet that might be exploited in such attacks. Importantly, we will work with and seek to influence government and governance bodies, including CPNI[2] and UUK[3] to assist in developing regulations, advice and guidance in such a way that benefits our customers.

We will also engage with and seek to influence national and international developments for activities that directly impact on our customers' end users in research, education, government and commercial programmes, ensuring product developments meet customer requirements. This will include working with industry partners to ensure their products work with our particular sector use cases as well as to share information on security threats as a means to minimising the effect of attacks on our community.

Building on existing research and development activities, including the co-design process[4], we will work with customers and their users to develop, innovate and pilot solutions that meet their requirements for service enhancements, support tools, or activities that could lead to new services.

We will continue to originate and relay security information to customers and will work towards using increased automation to deliver security intelligence to our community and routing information in real time to the people who can act upon it. This will enable us to provide a more effective and responsive service, applying our expertise where it can provide the most value to the community.

We will provide advice and assistance where it is asked for or needed. We will continue to be an exemplar of good information security practice and a trusted adviser for the sector. For organisation that are not engaging with us in any way we will provide encouragement, whilst ensuring that their responsibilities to the Janet AUP[5] and Security Policy[6] are upheld.

[2] Centre for the Protection of National Infrastructure – www.cpni.gov.uk

[3] www.universitiesuk.ac.uk

[4] http://www.jisc.ac.uk/research/funding

[5] https://community.ja.net/library/acceptable-use-policy

[6] https://community.ja.net/library/janet-policies/security-policy

Our service will be professional and non-judgemental. We will work with partners and customers to provide services and products that help our customers protect their users and assets. We will ensure that our services are coherent and easy to use for our customers while maintaining excellence in service delivery and value for money.

We will benchmark the sector benefit to customers from increased information security so that we can demonstrate the economic impact of responding or not responding to incidents, including highlighting how the severity of an incident can depend on timing – for example the damage to an HE institution due to an incident during clearing is obviously far greater than at other times of the year.

We will ensure that Jisc itself is an exemplar in the implementation and use of its own security products.

Details of how we will deliver this strategy can be found in the accompanying 'Jisc security products and services strategic plan'.