Cyber security strategy 2018-2021

Vision

By 2021 UK education and research organisations will be more cyber resilient, better able to respond to security incidents and have the ability to demonstrate an increased cyber security posture to enable the UK's education and research sector to be the most digitally advanced in the world.

Mission

We work to protect the Janet Network and connected organisations, to help you make the most of your Jisc membership. Our mission is to safeguard the current and future network and information security of the Janet network and of our members' networks, creating a secure environment for organisations 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 cyber security policy and to ensure continuity of business and we will continue to invest in shared services to protect the education and research sector.

Context

High profile cyber security incidents are mainstream news and awareness of the number and type of attacks has been growing year on year. Although Computer Security Incident Response Teams (CSIRT) including Jisc's were developed to tackle cyber attacks for research and education networks in the 90s, the environment in which we work has evolved significantly. Whereas most incidents were previously reported via email, we now receive the majority of information from automated systems. We receive considerably more information now – more than ten times as many incidents reported compared to 10 years ago – and the impact of attacks has also increased due to the increasing sophistication of attack tools, with 'attacks as a service' now commonplace.

Since our first security strategy was published in 2015 there have been many developments at both Government and international levels and this updated strategy now reflects the National Cyber Security Strategy 2016-2021[1]. 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.

Since we published our first strategy in 2015 we've achieved the following:

- Set up a Cyber security division – focussing all security related activities into one organisational structure.
- Established Jisc's Security Operations Centre – bringing together Janet CSIRT and DDoS mitigation functions into a single team alongside a new team of penetration testers.
- Established an in-house professional services team to provide a range of penetration testing and security assessment services, including red teaming and social engineering.
- Implemented a Vulnerability assessment and information service and a Phishing awareness and associated training service.
- Invested in a market-leading DDoS mitigation solution to reduce the time taken to mitigate attacks, increase our capability to defend against attacks and developed enhanced services that allow tailored and bespoke solutions that directly meet members' needs.
- Began the annual Cyber security posture survey to ensure we continue to provide services and products that our members' value.
- Launched the Cyber security portal to provide better visibility for our members of their network traffic and DDoS mitigations and alerts.
- Instigated the annual Jisc security conference
- Piloted the security x-ray service to help institutions identify their spending on security controls and provide targeted advice and guidance.
- We even launched our first cyber security documentary featuring some of our staff, members and partners highlighting how we help protect the Janet network and our institutions: https://www.youtube.com/watch?v=DpjoZGOONiQ.

[1] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

For the 12 months to June 2018, Jisc's Security Operations Centre (SOC) saw more than 1,300 DDoS attacks against its members and handled more than 6,000 other incidents or queries. In effectively defending members, our SOC analysts have witnessed an evolution in attack methods in an attempt to counteract the defensive measures that are now in place to protect colleges and universities.

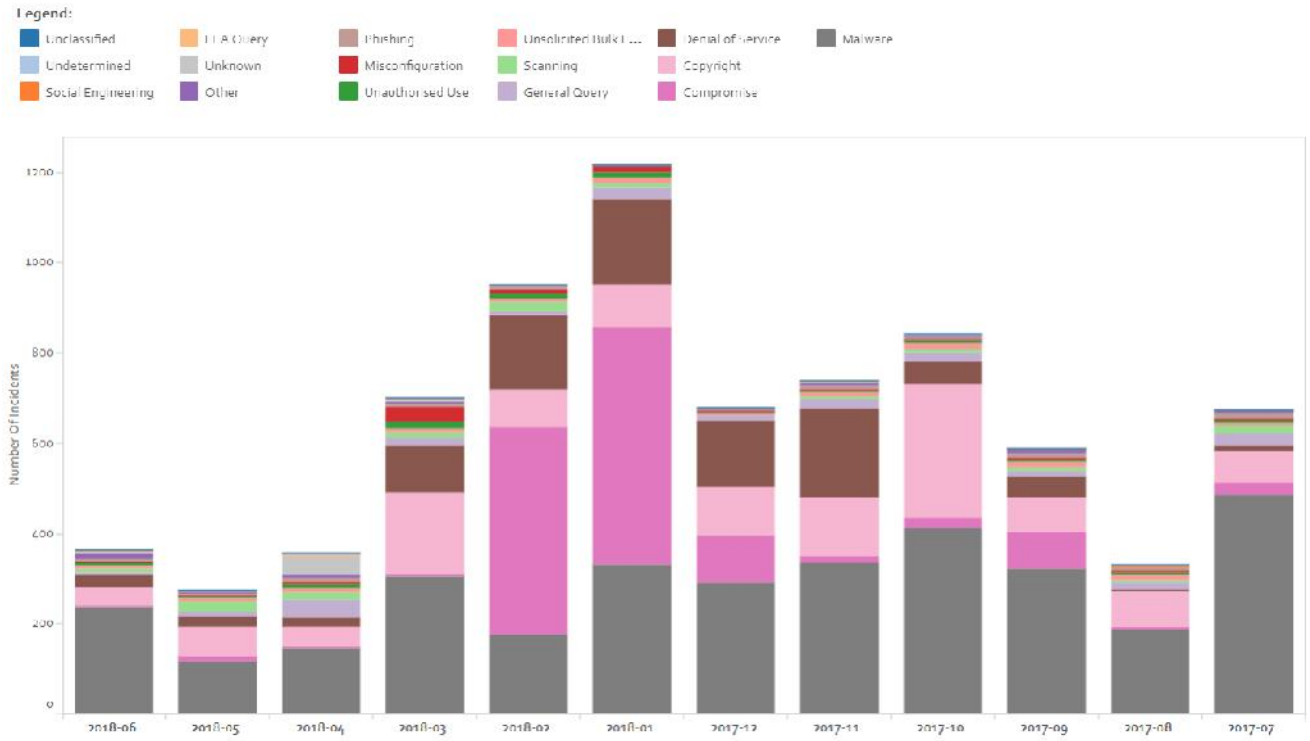

Figure 1. Incidents handled by Jisc's Security Operations Centre July 2017 - June 2018

Jisc, as a provider of shared services to education, provides not only the network connectivity, but also a comprehensive range of specialist security services tailored to the needs of the education and research sectors including proactive monitoring of user credentials being sold or traded online; alerting to the latest malware seen on the Janet network; and alerting and guidance on the latest outbreaks of phishing and ransomware campaigns e.g. WannaCry.

The Jisc SOC helps education and research institutions with the detection, mitigation, incident management and recovery from cyber security attacks. Ransomware and phishing incidents are a growing problem, recognised as the top risks facing the education sector. All these incidents could have caused significant impact to organisations, directly, or via fines or enforcement action from the Information Commissioner's Office under GDPR. Loss of sensitive student data also directly impacts student trust and leads to reputational damage to colleges and universities.

As the provider of the Janet network, and in being owned by our members, Jisc is in a unique position in being able to provide a comprehensive set of security products and services, including the central coordination of cyber threat intelligence from the tertiary education sector, across the Janet infrastructure, from National Research and Education Networks across the globe, and central coordination for security incidents.

What we do

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 aims to change the attitudes and behaviours of organisations and users of their networks. It also covers requirements on Janet-connected institutions to ensure Jisc is better placed to protect our member organisations and their students, staff and researchers.

To continue providing a world class service we will seek to enhance the customer and user experience through understanding their challenges and needs for cyber security and implementing robust services to respond to these needs no matter how large or small their organisation.

To assist members in assessing their security needs, we have mapped our services to the National Cyber Security Centre's 10 Steps to Cyber Security (https://www.ncsc.gov.uk/guidance/10-steps-executive-summary) as a framework for describing how the Jisc SOC works to protect colleges, universities and our other members. The Jisc membership subscription provides:

- Network security – protecting Janet network connections from DoS and DDoS attacks. There are no limits to the number or type of attacks that are mitigated. No restrictions are placed on the amount or level of support provided by our SOC analysts. Direct access is provided to SOC analysts for advice and guidance whether or not an organisation is specifically being targeted. A Security Portal[2] is provided to allow members to track the number and types of attacks seen at an individual and national level. Customisations are available at a low additional cost to help provide additional protection to specific parts of colleges critical infrastructure, for example Websites, DNS infrastructure and SIP Gateways.
- Incident management – unrestricted direct access to Janet Network CSIRT during and outside of ongoing incidents. This is the first point of contact for any institution that is experiencing a security incident and needs help, advice or guidance to prevent, recover from, or investigate a range of cyber security incidents, for example: compromise, ransomware, or phishing.
- Monitoring – Jisc SOC analysts proactively monitor for user credentials being sold or traded online; provide alerts related to the latest malware seen on the Janet network; proactively monitor for botnet activity originating from member organisations; monitor the Janet network for signs of malicious activity including ransomware, malware infections and illegal scanning aimed at identifying weakness in preparation for future attacks. The SOC analysts actively use probes and honeypot infrastructures to understand new types of attacks.
- Malware prevention – for known types of malware the Jisc SOC monitors connections to command and control servers and notifies members when we see or are notified of suspicious traffic.
- Secure configuration – scanning is undertaken to look for misconfiguration or problems associated with patch management focussed on high risk attacks.
- User education and awareness – access to regular gatherings of security professionals working in the tertiary education sector to share experience, expertise and best practice advice and guidance in an open, but confidential environment, through our annual security conference and a range of communication channels and outreach activities. In addition, we provide incident response training, collective security briefings, and access to security purchasing frameworks.
- Home and mobile working – access to secure federated wireless authentication services via eduroam.
- Set up your Risk Management regime – security assessment, penetration testing and security x-ray services are all available for a discounted rate and delivered by our in-house teams focussed on the education sector. Accredited training courses covering Cyber risk management, guidance for GDPR; and incident response management are also available.
- Removal media controls and Managing user privileges – accredited training courses covering development of information security policies are available. Penetration testing and security assessment services, including social engineering, 'red teaming' and in-house training are available to members at a discounted rate.

Implementation plan

To deal with the changing landscape and to achieve our vision we will align with the NCSC's approach to DEFEND the Janet network and our members, to DETER our adversaries and to DEVELOP our capabilities, all underpinned by effective national and international action.

[2] https://cybersecurity.jisc.ac.uk/dashboard

DEFEND

The CSIRT function within the SOC will continue to work closely with our community to detect, report, and investigate incidents that pose a threat to the security of our customers' information systems. We will continue to investigate other forms of network abuse such as spam and copyright infringement. Due to the global scope of incidents, we assist national and international law enforcement agencies in their investigations, connecting them to our trusted contacts within the community. Information security threats are not limited to particular networks or national boundaries, and we work with other CSIRTs across the UK, Europe and the rest of the world to manage and resolve incidents. We have built strong relationships with other security researchers and sources of security reports to ensure we provide members with a fast and effective response and will continue to work with other CSIRTs to develop best practices in incident response.

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 incident response community, to ensure we are aware of both technical vulnerabilities and information about specific hosts on the Janet network that might be exploited in such attacks. Importantly, we will work with and seek to influence government and governance bodies, including CPNI[3] and UUK[4] 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 members' 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.

More specifically we will build on existing threat intelligence capabilities to react faster to incidents and where possible to prevent incidents, by providing more targeted threat intelligence to our members at tactical, operational and strategic levels. One example of this is that we will work with 3rd party suppliers and in collaboration with other organisations such as major UK ISPs, Nominet and the National Cyber Security Centre (NCSC) in sharing Response Policy Zone (RPZ) feeds in the best interests of the public to assist in analysing criminal use of DNS. We will also, by end 2019, implement passive DNS to assist in the identification of the suspicious use of DNS data.

DETER

We will continue to work with the NCA, NCSC and other law enforcement agencies to detect and investigate cyber incidents, and where possible will see these through to prosecution. We will continue to harden Jisc's own services and systems to lessen our attack surface and will continuously test for weaknesses and vulnerabilities by undertaking regular scans and penetration tests.

In May 2017 we conducted our first ever cyber security posture survey among members. Giving us valuable insight into the varied defensive landscape in our sectors, we now have a greater understanding of our members' top security concerns, which will help shape our future decisions. We know, for example, that the use of vulnerability scanning to identify weaknesses in security is becoming the main way our members are testing their exposure to cyber risk. This has now become an annual survey to ensure we continuously deliver the cyber security products and services that meet our members' needs.

[3] Centre for the Protection of National Infrastructure – www.cpni.gov.uk
[4] www.universitiesuk.ac.uk

DEVELOP

We will continue to develop the Jisc Security Operations Centre by recruiting and training skilled individuals. By 2019 we will look to have developed our digital forensics capability to enable us to undertake more investigative work as part of ongoing incidents.

A growing area of interest is for Jisc to provide more managed security services. We will undertake research with a view to implementing a managed SOC service for members by 2020, working with institutions to develop a unique sector offering to help protect institutions in an increasingly difficult environment, both from the number of attacks and the scarcity of skilled security personnel.

We will also continue to develop our advice, guidance and training to help you increase skills at your institutions and, by building on existing research and development activities, 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.

Conclusion

Since our last Security strategy was published in 2015, the way Jisc delivers cyber security has changed considerably to reflect the ever-changing security landscape. It is likely that when this strategy is updated in 3 years' time we will have undergone even more change, as although the types of threats are evolving, they are not going away, and as funding changes within the education and research sector we will need to be more agile and innovative about how we all work together to address cyber security threats.

[5] https://community.jisc.ac.uk/library/acceptable-use-policy
[6] https://community.jisc.ac.uk/library/janet-policies/security-policy