Jisc security products and services strategic plan

Introduction

Jisc's security products and services strategy (2015 - 2018) outlines the high level objectives to help the research and education sector protect itself from network security threats and information loss. This plan describes how these objectives will be met over the next three years by bringing a range of security-related services into a coherent offering including information security and information security governance.

Both the security strategy and plan will be regularly reviewed to ensure we continue to meet customer requirements. To engage with Jisc in the area of information security, you can join the Security community group at https://community.ja.net/security. .

Services

To ensure our portfolio of security services continues to meet customer needs we will strive to maintain excellence in service delivery and value for money. To do this we have agreed the following targets to be achieved over the next three years.

Objective	Target
Benefits	We will investigate options for benchmarking the landscape to determine how improved security can help Jisc's customers achieve their strategic objectives. We will work with UCISA, UUK and international partners to identify ways to measure the benefits and demonstrate the value of security investments.
Coordination and cooperation	To deliver more effective and efficient proactive and reactive services by improving linkages nationally and internationally to best represent the needs of the research and education sector in the areas of information and cyber-security.
Representation	Represent the requirements of UK education and research through engagement at policy and regulatory levels.
Liaison and communications	We will establish a process of regular stakeholder liaison across the FE, HE, skills and schools sectors, including community experts. We will also consult with and engage with relevant non-sector bodies and organisations including CPNI, BIS and the Cabinet Office.
Training and awareness	We will help UK education and research organisations to protect their networks, people and assets by working with partners to increase capability through training and awareness including helping customers put in place the appropriate information security governance mechanisms.

Reactive Services

Reactive services are “triggered by an event or request, such as a report of a compromised host, widespread malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system” (http://www.cert.org/incident-management/services.cfm).

Jisc’s reactive services are designed to respond to requests for assistance, reports of incidents from the Jisc community and the wider Computer Security and Incident Response Team (CSIRT) constituency as well as those threats or attacks identified by Jisc itself.

Reactive services include, but are not limited to: Alerts and Warnings (received from the community, vendors, security experts etc.); Incident Handling (responding to specific requests and reports from the sector, and analysing incidents and events); Vulnerability Handling (receiving, analysing and dealing with information and reports about hardware and software vulnerabilities); and Artefact Handling (responding to files or objects found on a system that might be involved in probing or attacking systems and networks e.g. viruses, Trojan horses, worms, exploit scripts, and toolkits etc.).

We will disseminate information to any and all relevant parties about specific attacks, vulnerabilities, intrusion alerts, viruses, or hoaxes and provide appropriate recommendations to address the specific issue. This may take the form of initial short term actions to minimise the initial threat, and longer term actions to prevent similar issues. Jisc will also provide guidance on how to recover and protect any systems that were affected.

Any information gained by us from dealing with such issues may be distributed to partner organisations including vendors, other CSIRTs or security experts, or other parts of the community as a way to mitigate future similar occurrences. We will also seek to develop a robust situational awareness to ensure we have a timely and effective view of the risks and threats across all Jisc infrastructure and services allowing us to know when there is an issue (like Heartbleed or Bash), how it will affect us and our customers.

To continue providing a high level of reactive services we will start treating many security events as business as usual. The expectation should be that most customers have the capability to respond to these events in a mature fashion, rather than having them individually coordinated by CSIRT. Customers do not necessarily need closer guidance for the malware they see every day, therefore Jisc's default action will be to provide customers with details of security events directly and where appropriate in an automated way that will improve our service and responsiveness. The intention is that these changes will allow us to be more responsive when important events occur, and be more involved in the incidents that require CSIRT's expertise.

Janet CSIRT work closely with our community to detect, report, and investigate incidents that pose a threat to the security of our customers' information systems. We also 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 customers with a fast and effective response and will continue to work with other CSIRTs to develop best practices in incident response.

To get one-to-one advice on security systems and recovery from compromise, contact the Janet CSIRT Team via https://community.ja.net/library/janet-services-documentation/contact-csirt.

Proactive Services

Although reactive services have traditionally been the core component of CSIRT work, Jisc's security products and services strategy has an increased focus on proactive services. These services provide assistance and information to help education and research organisations prepare, protect, and secure their systems in anticipation of attacks or events in order to reduce the number of incidents in the future.

Proactive services are designed to help customers improve their infrastructure and information security processes before any incident occurs or is detected so that their impact is reduced when they do occur. A key part of this is ensuring the correct governance is in place so we will work with Janet-connected organisations to help you put in place the appropriate information security governance mechanisms that are appropriate for your organisation. Part of this will be to ensure organisations consider information security as part of their Business Continuity Planning strategy.

A core part of our service is the research, analysis and dissemination of security information. When sites connect to the Janet network, relevant contacts are automatically added to a UK-security mailing list to ensure they are kept informed of alerts, vulnerability warnings, and security advisories enabling them to protect their systems and networks against newly discovered problems before they can be exploited. In addition, it is recommended that relevant contacts also join the community site at https://community.ja.net/security. We also monitor legal developments and technological advances to extract relevant information for research and education customers as well as discovering new threats and trending areas through regular communication with other national and international bodies. This information is aggregated for dissemination to our community.

To help customers proactively protect their systems and users we provide content and web filtering services. We will shortly be procuring a new filtering service, but the current centralised web content filtering service provides protection against access to inappropriate content on the Internet. The web interface enables organisations to manage their own list of blocked or permitted URLs, filtering in accordance with local policies and can be tailored to match exact needs (https://www.ja.net/products-services/janet-connect/web-filtering).

The Janet Mailer Shield (https://www.ja.net/products-services/janet-connect/janet-mailer-shield) service provides a front end to an organisation's mail server, so it is not exposed to direct connections from compromised third party mail servers. The service also offers additional security by identifying the source of a message, indicating whether it is listed in selected DNS blocklists and adding a tag to indicate possible spam, helping to protect end users against unwanted email.

The Janet Spam-relay Tester and Notification System (https://www.ja.net/products-services/janet-connect/email-advice-and-testing) can test mail servers to ensure that they are secure against unauthorised message relaying, and will report any vulnerabilities found. The test involves connecting to a mailer and relaying a series of individual messages through it, just as the bulk mailers do in preparation for a spam run. The system will scan servers on request, however, we can also systematically run the test on Janet-connected systems which have been reported as relaying spam.

DNS blocklists and whitelists identify either sources of email abuse, or known 'good' email servers. Sites that have a Janet connection can have access to a number of leading DNS blocklists and whitelists via the Janet DNSBLs & DNSW service (https://www.ja.net/products-services/janet-connect/janet-dnsbls-dnswls).

We are working towards establishing a threat information service that will seek to aggregate threat information from commercial and academic sources to help provide better situational awareness for organisations connected to the Janet network. This information could be used to form part of your approach to cyber and information security. This service will also help you to adopt a risk-based approach to protecting information assets while helping to ensure this approach is rooted in the governance and management processes of your organisation.

More direct services that we provide include vulnerability testing and consultancy services designed to minimise the risk to organisations of significant information security breaches and reduce the associated costs of prevention, management, remediation and audit activities. We currently offer both automated accredited penetration testing and bespoke penetration testing as part of consultancy services that are tailored to meet your exact requirements.

Our services and products can help customers address the technical aspects of cyber security (protecting systems, networks and information), but to increase their security we also aim to help change the attitudes and behaviours of organisations and users of institution networks. To do this, we will establish a stakeholder group with representation across the FE, HE, skills and schools sectors, including community experts. We will also consult with and engage with relevant non-sector bodies and organisations, including the Centre for the Protection of National Infrastructure (CPNI), BIS and the Cabinet Office. As institutions increasingly widen their engagement with industry we will also seek to engage with industry as both suppliers and partners.

Reports from CPNI clearly state that there is a growing risk of cyber attacks from both criminals and nation states and CPNI has been involved with investigating a growing number of incidents involving universities. These attacks were in some cases sophisticated, but in other examples simple precautions, such as not plugging unknown devices into your laptop, would have prevented a number of incidents. This reinforces the argument for strengthened information security, rather than just 'cyber' security, and we will work with partners providing advice and guidance in this area, including the following to provide a coherent offering to help mitigate information security risk to the sector.

An example of such guidance is UCISA's Information Security Management Toolkit - http://www.ucisa.ac.uk/representation/activities/ismt.aspx, which we worked with UCISA and other partner organisations to write and review. The Toolkit will help senior management understand why information security is an important, organisation-wide issue and will provide advice and guidance to those who have responsibility for implementing information security across the organisation.

We also provide information on computer security issues through a range of training courses. A full list can be seen at https://www.ja.net/training and includes Effective Identification and Management of Security Incidents; Hands on Security Testing; and Information Security Policies. We will continue to develop training including determining the best route to provide guidance on iso27001 and liaising with international organisations to host appropriate training in a more accessible way for our customers.

Research and Development

To ensure our services continue to evolve to meet customer needs we undertake a programme of research and development both to enhance existing services and with a view to developing new services.

Co-design: Security

Co-design[1] is our collaborative innovation model. Steered by customer priorities, it is designed to exploit new opportunities and address pressing issues in higher and further education through technology. The co-design process enables us to draw on evidence to decide which challenges to focus on, invite experts to work on challenges and gather potential ideas, pursue promising ideas as projects, and to work with partners to ensure solutions address real problems and deliver real benefits.

Over the next three years we will be exploring products and services that will allow customers to improve their own incident response capabilities. We would also like to explore development of information/training for senior management (Executive Board members) that can help IT Departments make the case for Information Security internally and will also investigate developing dedicated infrastructure to support training and skills development.

We will continue to analyse attacks to better understand the threats, and to work with institutions to minimise their effects. We are actively exploring the most appropriate way to gather meaningful data from the network, allowing CSIRT to analyse and detect various types of threat even more effectively; this will allow additional actionable information to be distributed in a timely fashion to customer sites.

We will continue to implement temporary measures at the boundaries of the Janet network where this is the most effective way to mitigate the impact of attacks on customers. We will review the options for developing further proactive and reactive measures for both network-wide threats and site-specific ones. As part of an ongoing process to review the Jisc security products and services strategy and this plan, we invite suggestions for areas of information security that you need help in addressing and that could potentially be pursued through the co-design process.

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