Cyber security FAQs

Contents
General ............................................................................................................................................. 3
Why are we doing this? ......................................................................................................................... 3
I can look after my own institution’s security, why is the UIS getting involved? ....................... 3
How is the cyber security programme going to help me do my job? ........................................... 3
Why weren’t computer officers/IT managers in institutions asked for their expertise in this area before deciding to go ahead with this investment? ................................. 3
We’ve been fine until now – why do we need to spend a lot of money on new cyber security technology? ......................................................................................................................... 3
Who signed off such a big investment in cyber security? ................................................................ 4
Why are you forcing us to implement new systems when we’ve coped just fine ...................... 4
Why are we only being told about this programme now, when it started months ago? ................. 4
Who are the experts you’ve spoken to about this and when did you do it? ............................. 4
If this programme affects the entire University, why is the UIS running it without involving people who work in the University? ......................................................................................... 5
Why are we investing in so many different products? ................................................................. 5
Does all this mean we never need to worry about cyber security again? .................................. 5
I already manage cyber security really well – do I have to take part? ........................................ 5
Intrusion detection system ................................................................................................................. 7
Why do we need an intrusion detection system? ............................................................................. 7
How does the intrusion detection system work? ............................................................................ 7
What are the negative impacts of putting in an intrusion detection system? ......................... 7
Will the intrusion detection system read all my emails? ............................................................... 7
Will you be monitoring all traffic in and out of my institution? ................................................... 7
Can the UIS see my web browsing activity? .................................................................................... 7
Intrusion prevention system ............................................................................................................. 8
Why do we need an intrusion prevention system? ......................................................................... 8
How does the intrusion prevention system work? .......................................................................... 8
How will you know what settings to use for the intrusion prevention system when you set it up for my institution? ................................................................................................. 8
What are the negative impacts of putting in an intrusion detection system or an intrusion prevention system? ................................................................................................. 8
Will the intrusion prevention system read all my emails? ............................................................ 8
What information will the intrusion prevention system monitor? ......................... 8
Will the intrusion prevention system decrypt my private communications? .......... 9
Who do I contact if I have a question or when a problem occurs? ..................... 9
Who has access to the intrusion prevention system? ....................................... 9

Managed firewall service .................................................................................. 10
What’s the point of having a managed firewall service? .................................. 10
How much profit do you expect to make from the managed firewall service? ...... 10
Will the managed firewall service replace what institutions already have in place?
.......................................................................................................................... 10
Can the UIS adopt our institution’s current firewall? ...................................... 10
Is the managed firewall service a direct replacement for FireRack? .................. 10

Anti-distributed denial of service (DDOS) ......................................................... 11
What is Cloudflare and what does it do? ......................................................... 11
Why are we spending money on anti-DDOS software? ................................... 11
General

Why are we doing this?
With cyber-attacks becoming ever more sophisticated and coordinated, we want to protect the University’s assets and systems, staff members’ intellectual property, and all of the data and information we hold about both staff and students. To do this we are implementing a multi-layered approach to cyber-security that will help to protect these areas.

Back to top

I can look after my own institution’s security, why is the UIS getting involved?
We recognise a number of institutions do an excellent job protecting their systems and assets, however this is not consistent across the University. The UIS is also responsible for enhancing security across the entire collegiate University, looking beyond an individual institution to protect key shared infrastructure (such as the network) and services (such as Raven). The UIS team will work with institutions to make sure that they receive a solution that is tailored to their specific needs should they wish to use our new services.

Back to top

How is the cyber security programme going to help me do my job?
The cyber security programme will protect users and University assets from cyber-attacks in a variety of forms. The multi-layered approach is being implemented and should work almost invisibly to most people. People providing IT services within institutions will be able to ensure their institution is better protected and can receive guidance and expertise from the UIS security team.

Back to top

Why weren’t computer officers/IT managers in institutions asked for their expertise in this area before deciding to go ahead with this investment?
With a programme as broad as this, it is not possible to involve everyone we would like, however we did work with a number of security experts. These experts were drafted from areas such as the University’s computer lab and from external organisations and were involved in helping us to decide our approach to cyber security.

Back to top

We’ve been fine until now – why do we need to spend a lot of money on new cyber security technology?
While a number of institutions within the University do an excellent job at protecting their information and assets, the increasing sophistication of cyber-attacks means that we need to increase the amount of protection we have in place. We do know of instances where cyber-attacks have been successful and introducing and
implementing a multi-layered approach to cyber security will help defend the University against future attacks. The potential financial and reputational risks if we don’t invest in this area far outweigh the investment we are making.

Who signed off such a big investment in cyber security?
The Information Services Committee understood that the increasing sophistication of cyber-attacks meant we needed to increase the level of cyber security we have in place for the University and asked for the cyber security programme to be implemented and the Information Services Committee approved the actual budget.

Why are you forcing us to implement new systems when we’ve coped just fine until now?
While some parts of the University manage cyber security very well, a number of other areas have expressed the need for help when it comes to addressing cyber security risks. The new tools that the UIS is introducing, namely the anti-DDOS service and the intrusion detection system, should have no functional impact on systems, but will offer additional layers of protection against cyber-attacks. The intrusion prevention system will not be implemented without close consultation with individual institutions to ensure it meets their specific needs.

Why are we only being told about this programme now, when it started months ago?
We have been working with a number of individuals and groups across the University in the development of this programme, however we have only recently had outcomes that we could communicate. We will continue to provide relevant updates as the programme progresses.

Who are the experts you’ve spoken to about this and when did you do it?
With a programme as broad as this, it is not possible to involve everyone we would like, however we did work with a number of security experts. These experts were drafted from University committees and sub-committees, the computer lab and from external organisations and were involved in helping us to decide our approach to cyber security and which products we would implement.

When will all this be implemented?
There are four different phases to this programme. The first phase involved a great deal of background work, including a lot of analysis, testing and system design. The second phase, which is what we’re currently working on, involves the
implementation of many of the cyber security tools and the introduction of online training. This will continue into the third phase, which will also see the introduction of the intrusion prevention system for the UIS. The fourth phase will involve, among other things, consultation and implementation of the intrusion prevention system for institutions.

If this programme affects the entire University, why is the UIS running it without involving people who work in the University?
The UIS has worked with individuals and groups from across the University, including the Information Services Committee and experts from the Computer Lab to plan and execute this programme. When it comes to implementing the intrusion prevention system, programme team members will be consulting and working closely with institutions to ensure the system is configured to meet their individual needs. Some cyber security products will only work if they are located on the backbone network in specific locations, which means the UIS needs to manage them centrally.

Why are we investing in so many different products?
With cyber-attacks becoming ever more sophisticated and coordinated, we want to protect the University’s assets and systems, staff members’ intellectual property, and all of the data and information we hold about both staff and students. No single solution will protect the University from every type of cyber-attack, so the UIS has identified a variety of products to address different areas of vulnerability. Implementing this multi-layered approach will help to protect the University, its assets and staff to make sure that there are different levels of protection to enhance the security of our systems.

Does all this mean we never need to worry about cyber security again?
While it would be nice to say that the approach we are taking to cyber security is a remedy for everything and that we don’t need to worry about it once the multi-layered protection is implemented, this is simply not the case. These new systems will mitigate much of the risk, however individual institutions will still need to ensure they continue to update, patch and maintain security tools to ensure they keep as up-to-date as possible to combat security threats.

I already manage cyber security really well – do I have to take part?
With cyber-attacks becoming ever more sophisticated and coordinated, we want to protect the University’s assets and systems, staff members’ intellectual property, and all of the data and information we hold about both staff and students. To do this we are implementing a multi-layered approach to cyber-security that will help to protect these areas. As some of the solutions we’re implementing sit either at the
network edge or boundary, institutions will receive the benefits of additional layers of protection, although they should see no functional change to their systems. When it comes to the way in which the intrusion prevention system operates, institutions will be consulted directly and at length to establish how they would like the system configured to ensure it meets their individual needs.
Intrusion detection system

Why do we need an intrusion detection system?
As cyber-attacks grow more sophisticated, gaining a clear understanding of the nature and frequency of threats the University faces becomes increasingly important. The IDS will help us understand the nature of these threats and help us to prepare for and mitigate the risk and impact resulting from cyber-attacks. This system, which the CamCERT team will administer, will detect a variety of serious threats and will notify institutions about them so they can take immediate action. This will lower the risk associated with any cyber-attacks.

How does the intrusion detection system work?
The intrusion detection system simply monitors traffic as it passes into and out of the University’s network. It doesn’t actively stop attacks or threats; instead it alerts that there is a possibility that some traffic is considered a threat based on its configuration parameters. The intrusion detection system is automatically updated to recognise the latest attacks and vulnerabilities using a commercial subscription from a leading solution provider.

What are the negative impacts of putting in an intrusion detection system?
There should be very little in the way of negative impacts. The intrusion detection system will simply monitor the traffic going through the networks and flag any item that looks suspicious. It does not take any action.

Will the intrusion detection system read all my emails?
No.

Will you be monitoring all traffic in and out of my institution?
The intrusion detection system monitors traffic between the University’s network and the internet (Janet), however it simply detects cyber threats and reports them; it doesn’t take any preventative action. CamCERT will receive alerts about serious threats, which will in turn contact the relevant institution to take action.

Can the UIS see my web browsing activity?
The intrusion detection system monitors URLs to ensure there is not a cyber security threat and, if a threat is raised, the CAMcert team will be alerted and will pass this along to the relevant institution. At no time will user identifiable data be monitored.
Intrusion prevention system

Why do we need an intrusion prevention system?
The IPS complements the intrusion detection system however it won’t be implemented immediately. The UIS will start to use it after the intrusion detection system is in place, which should take place in January 2017. This system will act as another line of defence and help protect systems, information and data. It will be implemented in consultation with individual institutions and can be configured to meet their specific security requirements.

How does the intrusion prevention system work?
The intrusion prevention system is the same system as the intrusion detection system and once it is functioning it will drop packets it has been configured to recognised as cyber threats in addition to providing alerts.

How will you know what settings to use for the intrusion prevention system when you set it up for my institution?
We aim to develop a standard set of security parameters around installation, which will involve consultation with institutions. These will be tested using the detection policy and only switched to prevention once false positives (i.e. when packets that should go through but are dropped) have been minimised. This work will be done in consultation with institutions.

What are the negative impacts of putting in an intrusion detection system or an intrusion prevention system?
An intrusion prevention system drops packets, which will inevitably lead to a few false positives, especially as we fine tune the system. The CAMCert team will fine tune the policies before switching on the prevention mode, and will monitor the system actively once prevention policies are in place.

Will the intrusion prevention system read all my emails?
No.

What information will the intrusion prevention system monitor?
The intrusion prevention system is the same system as the intrusion detection system, so it monitors the same information. The difference lies in the fact that the intrusion prevention system will drop packets it perceives as a cyber threats. As this system is highly configurable, the kinds of threats it will take action against will be
determined at an institutional level in partnership with the UIS, which gives institutions the ability to configure it according to their individual needs.

Will the intrusion prevention system decrypt my private communications?
No, decryption will not be used.

Who do I contact if I have a question or when a problem occurs?
CamCERT will manage the IPS, which can be contacted at cert@cam.ac.uk.

Who has access to the intrusion prevention system?
Two teams within the UIS managed the intrusion prevention system; the Network Systems team, which assists with network-level configurations; and CamCERT, which assists with security configuration and incident response. Other UIS staff may request information logged in the IPS, but this is controlled and limited to appropriate individuals.
Managed firewall service

What’s the point of having a managed firewall service?
Simply speaking, the managed firewall service gives institutions the flexibility and freedom to deliver an additional layer of protection to their institution without needing the resource or knowledge in-house.

How much profit do you expect to make from the managed firewall service?
There are no plans to make a profit at all. The pricing for the managed firewall service has been calculated to make sure that its running costs are covered and to cover a full replacement in four years’ time.

Will the managed firewall service replace what institutions already have in place?
As the service is optional, it depends on what services institutions are already running, however the service has been designed to remove responsibility for managing the firewall from the institution to the UIS. This means that in many cases scarce resources can be redirected to other areas that require attention.

Can the UIS adopt our institution’s current firewall?
If the institution’s firewall is a model Fortigate currently supports, the UIS may be able to adopt it. Please contact Ashley Culver to discuss options.

Is the managed firewall service a direct replacement for FireRack?
No, it is a complementary service that can sit alongside FireRack and work with it to provide layered protection against cyber-attacks.
Anti-distributed denial of service (DDOS)

What is Cloudflare and what does it do?
Cloudflare is a cloud-based solution that offers protection against distributed denial of service (DDOS) attacks. It sits at the network edge to mitigate the risk DDOS attacks pose.

Why are we spending money on anti-DDOS software?
Distributed denial of service (DDOS) attacks are not a recent phenomenon, however the methods and resources used to carry out and hide such attacks have evolved a great deal. The University's international reputation makes it a prime target for DDOS attacks, which have the potential to cause severe reputational harm. We are implementing anti-DDOS services to mitigate some of the risk these kinds of attacks pose.