PRESENTER: With growing amounts of cybercrime out there, what does it mean for your pension? Well to discuss that I'm joined now by Claire Barnes. She's an associate and senior pension management consultant at Barnett Waddingham. Claire, if there's growing amounts of cybercrime, there must be equal and opposite, cybersecurity. So can you give us a working definition of cybersecurity? CLAIRE BARNES: Yes. Cybersecurity is the practice our defending our computers, software, networks, personal devices and data against any malicious attack. PRESENTER: But there's cybercrime in lots of places, why are pension schemes a particular target? CLAIRE BARNES: So UK pension schemes hold millions of member records, trillions in assets, and therefore they're becoming an increasing target for cyberattacks. These attacks may be external attacks, so for example criminal, cybercriminals or terrorists, or they may be internal attacks, for example insider attacks. So therefore I think trustees really need to assess this risk on their scheme and take steps to protect members' information, and also their assets and cash that they hold. PRESENTER: So what can trustees put in place to reduce this cybersecurity risk? CLAIRE BARNES: So trustees need to identify, evaluate and manage cybersecurity risk as part of their internal controls. So I'll just go into a bit more detail on those three steps. So when they're identifying the risk, the sort of cyber risks that may occur in a pension schemes are things like the risk that data is sold on the black market, or fraud from identity theft, or maybe from an administrator from clicking on that unverified attachment. So trustees need to be able to assess this risk. So they need to ask themselves do they understand the risk, have they had training on the risk, do they know the functionality of their systems and procedures, and finally have they got access to the right sort of expertise. The second step is evaluating the risk and adding controls around that risk. So cyber risk needs to be managed across all parties of a pension scheme. So that includes the trustees, investment managers, administrator, adviser and employer. And what you might tend to do is send a questionnaire out and ask the individuals around the particular cyber risk element. So for example you might ask the employer what are their controls around data? You might ask the same question to the administrator, as well as asking them what standards and accreditations they have to demonstrate their cyber readiness. As part of this they also need to set up an instant response plan. So this plan will detail what happens if the worst case scenario happens so that there's a response team that will notify the trustees or the chair as soon as the incident occurs. Then you follow the process to be able to notify the relevant regulators. And finally this plan will detail the management around the incident, to ensure that normal procedures are up and running as soon as deemed safe to do so. And then the final point is managing the risk. So once you've got the controls in place, testing these controls, testing your readiness plan, and also making sure that you're up to date with any governance and guidance around cybersecurity and that you're processes reflect this. PRESENTER: And what can advisers do to help trustees? CLAIRE BARNES: So advisers can help with training, as I mentioned, or putting together a questionnaire. They can also help with maybe doing an independent assessment of your cyber management. Or they may help with drafting the incident response plan, or looking at any cyber policies or data policies that you may have. PRESENTER: And how regularly should you review what your policies and procedures are around this, because the digital world moves so quickly? CLAIRE BARNES: I think the simple answer to that is that it should be on trustee meeting agendas definitely immediately. And then it should be reviewed as and when you feel that it's required. Definitely on an annual basis, but if there's any other events that's come up that makes it topical then it should be added. I think adding it to the risk register and reviewing it when you review the risk register is a fundamental part. PRESENTER: And final question, what are the penalties that could be involved for trustees if they're not up to speed with this as an issue? CLAIRE BARNES: So I think the whole aim of doing this is making sure that members' data is protected and their benefits are protected. So I think one would argue the main penalty is the impact on members, losing the trust of members and ultimately the reputational risk on the company. The regulator may also get involved if they deem that your controls are inadequate. And finally the financial risk. So last year

GDPR brought in a fine of up to 4% of your annual global turnover. So I think with cybersecurity it's such a hot topic at the moment. And it's an increasing risk, evolving risk, so therefore it's really important that trustees review the risk on their pension scheme. And I think this is evidenced by the regulator's guidance that was published last year. PRESENTER: We have to leave it there. Claire Barnes, thank you. CLAIRE BARNES: Thank you.