"An introduction to NCSC"
Cub Llewelyn-Davies, Charity Sector Lead, National Cyber Security Centre (NCSC)

The National Cyber Security Centre wants to support a special interest group of Charity IT Leaders on information and cyber security, its charity sector lead told delegates at the conference.

In his session, Cub Llewelyn-Davies gave a brief introduction to the NCSC before running through the types of cyber threats that are most pertinent to the charity sector, and the tools and guidance available to charities to help protect themselves against these.

The NCSC is the government agency responsible for cyber security in the UK, and its mission is essentially "to make the UK the safest place to live and work online".

It benefits hugely from being part of the intelligence agency GCHQ, Cub said. "Our understanding of cyber crime and cyber attacks have increased dramatically since we came together as one organisation."

He said that as well as increased threats from powerful nation states, particularly "an aggressive Russia seeking political advantage", "Chinese cyber attacks on our commercial interests", and intrusions from North Korea and Iran, the UK faces a growing threat from "people who attack just wherever they think there is money to be made".

He related an anecdote about an ex-offender named Carl who presented a session at another conference he was at recently, confessing how he had stumbled across a YouTube video which taught him how to buy lists of passwords off the internet. He used these to penetrate various reward programmes and sold the rewards on eBay for a little less than market value, before discovering he could buy software that automated much of this activity. Carl allegedly made £150,000 in nine months from this scheme while also holding down a full-time job stacking shelves in a warehouse.

"It doesn't take a genius to do cyber crime any more," Cub advised. "We talk a lot at NCSC about nation states but really there are a lot of people out there with very low sophisticated capabilities that are exploiting things that have been the same for a very long time. They rarely attack anything of strategic national significance but cumulatively these attacks amount to a direct challenge to our ability to have a thriving digital economy."

He said charities are particularly vulnerable to three types of attack:

- Ransomware, an attack that essentially cripples part or all of your networks. "If you haven't got decent back-ups, these types of attacks can leave you down for days, and potentially in a state that you can't really recover from."
- Business email compromise, where criminals send emails purporting to be from internal or external contacts requesting that you change bank account details or other corporate data. "Charities have transferred, in some cases, significant amounts of money into the hands of criminals while thinking that they were just doing their jobs."
- Credentials-stealing malware. "Credentials-stealing malware is gathering substantial amounts of data that can be used to enable a future cyber crime or fraud."

Cub said that for most of its existence, NCSC had focused its efforts mainly on small charities with less than £1m income who only need to apply a few simple or low-cost measures to enhance their cyber resilience. But lately the agency had turned its attention to larger charities.

As part of this, it has launched a toolkit to help trustee boards get to grips with cyber security. Cub asked the conference how many delegates had briefed their board on cyber security or information security. When about two-thirds put their hands up, he asked them how many were confident that the trustees had understood what they said and asked intelligent questions about the briefing. No hands went up.

“I’m afraid that is quite typical,” Cub said. “I think boards, whether in the commercial or charity sector, are on top of issues like pension liabilities or health and safety, things that have been on their agenda for a number of years. But they don’t understand cyber security, or even technology as a whole, because we’ve never really made it easy for them to.”

The toolkit is designed as modular guidance that allows trustees to delve into different areas and includes 25 questions they can ask their executive team. Themes range from asset control to how they are developing their staff awareness culture; from how they are bringing in new technology to what’s being done to ensure they are secure.

“But the key bit is that it also gives them the types of answers they should hear back,” said Cub. “So if they ask you ‘what are we doing to limit control of our most sensitive data?’, and they don’t hear something back around having a tiered access system where only those who need access to it have it, then they should delve further into that topic.” He said the Charity Commission is now promoting the toolkit as guidance for trustees of large charities.

NCSC has also launched an exercise box, which is a free tool that provides technical simulations for various off-the-shelf attacks and breaches so that charities can practise how to respond and boost their resilience. “It allows you to plan for cyber security incidents in the same way you plan for other risks such as a fire or flood, or a number of your staff doing down with flu this winter.”

Lastly, the agency has created ‘top tips for staff’, a free 20-minute e-learning resource for staff, trustees and volunteers on their roles in improving cyber security. “It’s fairly universal as it’s for businesses and charities so the language won’t be too specific, but it teaches little things like how to spot the obvious signs, how to set a strong password, and how to report a phishing email if they get one. These are getting much harder to spot; we’ve moved beyond the days where it’s a prince you’ve never heard of from a faraway land offering you an inheritance.”

Cub concluded his presentation by proposing to delegates that if members of Charity IT Leaders were willing, NCSC would like to support a special interest group around information security and cyber security. He said that increasingly his team are being asked whether there are any forums where people can be open and honest about their cyber security challenges and not be made to feel stupid by others who claim to have achieved gold standard. “We’d really like to support something along those lines if there’s an appetite for it,” he said.

Anybody wishing to get involved in such a special interest group should email tree.hall@charityitleaders.org.uk