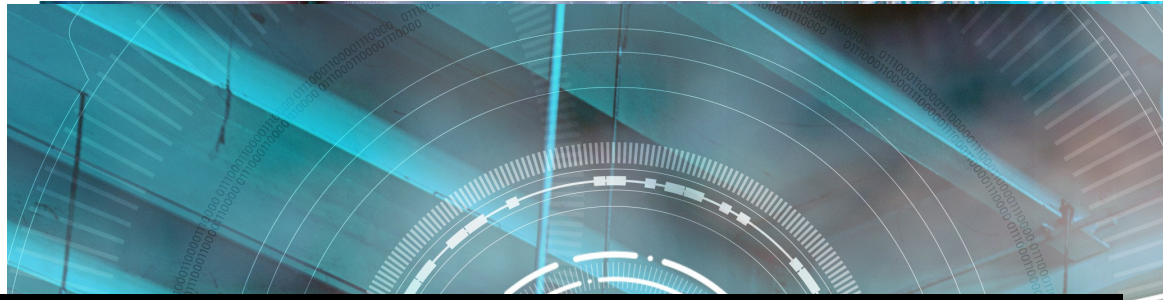


SMALL AND MEDIUM SIZE CHARITY

CHARITY CYBER SECURITY LEADERSHIP AGENDA

RAISING CYBER SECURITY CONCERNS WITH TRUSTEES AND THE LEADERSHIP TEAM

CLASS NETWORKS

Cyber Security is now top of mind as a business-critical topic for most leaders of small and medium size charities and voluntary organisations. As a whole, the sector is increasingly aware that it's not just larger organisations that are targets for hackers, malware and cyber-attacks.

The recent Charity Commission report, "Taken on Trust: The awareness and effectiveness of charity trustees in England and Wales, acknowledges that charity trustees "recognise the threat from fraud and external cyber-attack but remain concerned about their own skill proficiencies in this respect."

The Report also highlights the case that a significant minority of trustees from the smallest charities (do not regard it as applicable to them and remain less aware of the risks of cyber-attack. The report concludes that there is a need for additional customised training and support to promote greater skills amongst trustees in the monitoring and implementation of measures to protect against fraud and cyber-attacks.

Given the scope and complexity of the issue – in the face of a small staff and limited resources – how do you start a conversation with your trustees and leadership team about how to best address your organisation's needs? Below are suggested questions and topics you can use to help guide a conversation about your current cyber-security posture and cyber-security best practices.

OVERVIEW OF CYBER THREAT

Consider providing a threat briefing to update your team on the current cyber threat environment, especially in the context of the particular concerns of Third Sector small and mid-size organisations.

UNDERSTANDING RISK

Facilitate a discussion about how your organisation uses information technology (IT) to support your core culture and functions, how you allocate and support cyber security resources, and how you maintain and improve your state of readiness:

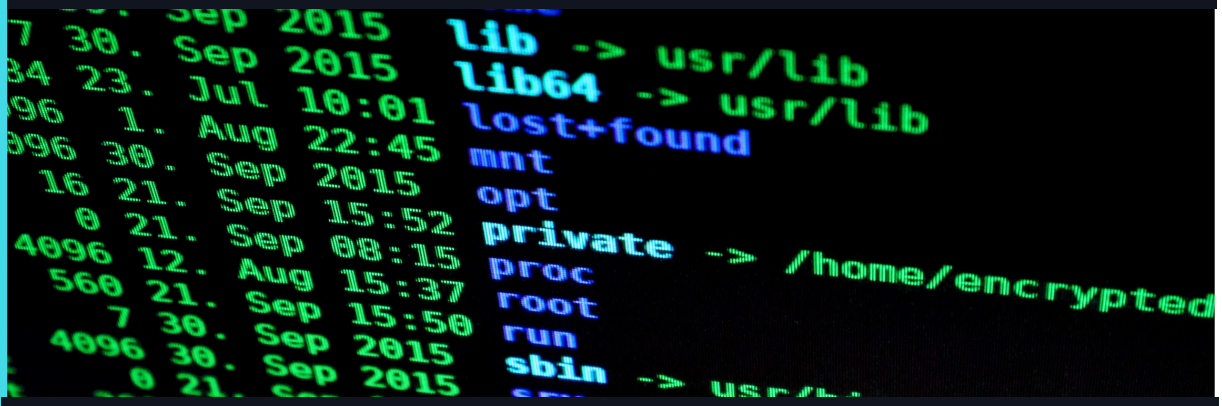
· Are you restricting the use of email to communicate with donors, fundraisers and sponsors?

· Do you have concerns about engaging with service users and donors using social media, especially in the light of Facebook sharing data with private companies? recent Companies?

Is the fear of cyber attack preventing you from innovating?
· Would you like to fundraise using social media?
ear of cyber attack preventing you from innovating?
· Would you like to fundraise using social media?

QUESTIONS ABOUT OUR ORGANISATION

1) What does our organisation value?
2) What are the core functions or services that our organisation provides?
3) What are our most valuable information assets and who might want them?
4) What are the potential confidentiality, availability, or integrity impacts to clients and sponsors of our services?
5) How does connectivity with our partners, subcontractors, or vendors affect our cyber risk?
6) Do we collect and/or store sensitive Personally Identifiable Information (PII) and/or health data, information on minors?



QUESTIONS ABOUT OUR RESOURCES

1) Do we have the proper staffing and resources to protect our information and cyber infrastructure? With the GDPR regulations coming into effect in May, it is essential that you start a process of data analysis and management. If not,
a. What resources are we able to allocate toward improving our internal capabilities?
b. What external services can we access, or which organisations can we partner with to secure these capabilities?
2) How are decisions made for cybersecurity and resource allocation?
3) How are we informed about industry trends and new technologies?
4) How are risks communicated across the organisation?
5) Is our leadership team regularly informed about the level of cyber risks to our organisation?

QUESTIONS ABOUT OUR PREPAREDNESS

1) What are the biggest challenges our organisation faces in managing our cyber security?
2) What are the potential health, safety and environmental risks to our organisation if we face a cyber-attack?
3) Do we have robust incident response policies and procedures in place to react swiftly to a cyber-attack? How often are they tested/audited and updated?
4) What are our financial, competitive, reputational, and regulatory risks?
5) With which external organisations do we share our data?
6) Do we have the proper agreements and safeguards in place to protect ourselves?
7) Have we formed partnerships with the relevant providers, within our sector, or with cross- sector partners to better coordinate security efforts?

EXISTING ORGANISATION SECURITY PLANS

Discuss the state of existing organisation security plans with your Trustees and leadership team.
1) When did we first develop our plans, and when did we last update them?
2) Do our plans address cyber risk management and physical risk management?
3) Who should review the plan(s), both internally and externally?
4) How will we communicate the information in the plan(s) to our employees and volunteers to ensure compliance?
5) Do our plans address the questions in the sections above?

NEXT STEPS FOR OUR ORGANISATION

Discuss next steps for your organisation based on your current cyber security posture.

1) Which are high priority areas for immediate action?
2) Will we revise our short, medium, and long-term security goals based on our current cybersecurity posture?
3) How often will the leadership team meet to discuss company cyber security?

SOURCES

"Taken on Trust: The awareness and effectiveness of charity trustees in England and Wales, The Charity Commission, November 2017

DISCUSSION OF RESOURCES

Discuss which cyber risk management resources would be beneficial to your company.

Providers such as Class Networks can conduct an impartial risk analysis and recommend processes, risk management tools and resources geared specifically towards the needs of charities and voluntary sector organisations.

0800 160 1920
contact@cassnetworks.com
www.clssnetworks.com

CLASS
NETWORKS