PASA Cybercrime and Fraud Working Group

Produced in partnership with:

Crowe

PASA Experts for Cybercrime & Fraud

PASA Cybercrime Protection Checklist

May 2022

PASA Cybercrime Protection checklist

Acknowledgments

PASA is grateful to the authors of the Guidance and members of the PASA Cybercrime and Fraud Working Group (CFWG) and their employers.

Paul Sturgess (Board Sponsor)	**PASA Board Director**
Jim Gee (Chair)	**Crowe – PASA Experts for Cybercrime & Fraud**
Andy Cassin	**WTW**
Gillian Baker	**Hymans Roberston**
Justin McLelland	**Stephenson Harwood**
Kate Whitford	**Stephenson Harwood**
Michael Walters	**Invensys Pension Scheme**
Philip Goodchild	**Stephenson Harwood**

1. Introduction

The **PASA Cybercrime Guidance** published in November 2020 provided administrators with background information on cybercrime, described how it's evolved over time and discussed the protection measures which could be considered to:

- Meet Legal and Regulatory Standards
- Understand your organisation's vulnerability to cybercrime
- Ensure your organisation is resilient to cybercrime
- Remain able to fulfil key functions

This checklist provides examples of steps administrators can take to assess their defences against cybercrime in these four areas. These examples are by no means exhaustive and we encourage each administrator to add any further items you feel are especially relevant to your environment. Unfortunately, even by following all the steps suggested in this document, it may not prevent a successful cyber attack.

Before considering the checklists in each area, you should take the following steps to establish your scope and coverage:

1. Appoint a named individual with overall accountability for cyber security and resilience, as well as relevant team members who have day to day responsibility in defined areas
2. Analyse and understand your data, systems, applications, premises and process flows – and how they integrate with your business operations
3. Understand the different people and groups you interact with – such as employees, contractors, temporary workers, suppliers, clients and members
4. Consider who will be responsible for using the checklists to assess your cyber security and resilience readiness, both in the initial review and any follow up, to ensure independence is maintained

2. The Checklists

Meet legal, regulatory and industry standards

- ✓ Review all relevant legislation (such as Data Protection laws) in the jurisdictions you operate in on an ongoing basis to understand what's required to achieve and maintain compliance
- ✓ Remain up to date with regulatory requirements and Guidance (such as from the FCA, TPR and ICO)
- ✓ Consider alignment to a widely recognised, risk-based Cyber Security or Information Security standard or framework (such as **ISO27001**, **NIST** or **ISF**) to avoid 're-inventing the wheel' when going more deeply into your Cyber controls assessment

Understand your organisation's vulnerability to cybercrime

- ✓ After an initial high level review, conduct a deeper analysis of your various vulnerabilities to Cybercrime, documenting both the process and outcomes – and commit to repeating it at least annually
- ✓ Assess how attractive your organisation might be to cybercriminals and what damage might be done if an attack takes place, rather than simply looking at the quality of your technical controls
- ✓ Input the outcomes of the steps above into your business risk management processes to ensure the correct decisions are made for cost effective improvements and to accept appropriate levels of residual risk
- ✓ Ensure quality by appointing individuals with relevant skills and experience. The appointed individuals should also have a degree of independence from those currently responsible for Cybercrime protection to demonstrate objectivity.

Ensure your organisation is resilient to cybercrime

- ✓ Follow Guidance from bodies such as the **National Cyber Security Centre** (NCSC) to stay abreast of the latest threats and vulnerabilities being exploited – but be aware even the most well-protected organisation is at some level of risk from Cybercrime
- ✓ Document a clear and accessible process, known by all employees, for raising any suspicion of a security incident – as well as a documented and tested plan detailing how you'll respond in the event of an attack
- ✓ Ensure those individuals/roles who would be affected know and understand their responsibilities and are suitably trained to fulfil them if an attack occurs
- ✓ Where necessary, have specialist services engaged and on call to supplement your in-house teams in the event of an attack
- ✓ Check your plan addresses all aspects of an attack, including minimising reputational damage, assisting the Data Controllers to comply with reporting requirements and protecting affected data subjects such as pension scheme members

Remain able to fulfil key functions

It's critical administrators ensure they have appropriate measures in place to maintain the delivery of the following key services reliably and securely in the event of a Cybercrime attack and immediately afterwards. These services include:

- ✓ Paying pensions, lump sums and death benefits
- ✓ Processing contributions
- ✓ Allocating/disinvesting monies to/from investments
- ✓ Answering enquiries by telephone, post, email or via websites
- ✓ Transferring accrued benefits to another pension scheme/provider
- ✓ Managing scheme bank accounts/payments/receipts
- ✓ Issuing member and employer communications
- ✓ Using their systems to look up information and update records
- ✓ Keeping accurate membership and accounting records
- ✓ Keeping up to date with pensions, tax and data privacy laws

3. Conclusion

Cybercrime was growing rapidly before the advent of COVID-19, but it's since surged with the Office for National Statistics recording a 113% increase in incidents. Organisations can't expect to be immune from cybercrime, but you don't have to be a victim. Administrators can be cybercrime resilient by being as well protected as possible, able to manage an attack when it occurs and able to investigate what's happened and recover and mitigate any damage.

PASA

assess | aspire | achieve

Get in touch:

info@pasa-uk.com

www.pasa-uk.com

PASA is a Community Interest Company and our full name is Pensions Administration Standards Association CIC. Company number: 6597097