Prepare your business: Checklist

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

CyberScotland
CYBERSCOTLAND PARTNERSHIP

Cyber and Fraud
Centre Scotland

Prepare your business: Checklist

Use this checklist to help prepare for, respond and recover from cyber incidents. For more information visit: https://www.cyberscotland.com/incident-response/

Plan ahead: What could you do to protect your business?	Notes
Identify and prioritise your most valuable assets □ What do you care about most? □ What are your 'Crown Jewels'? **When an incident occurs:** □ Consider your order of system recovery and prioritise these areas. □ Review at the time of invocation of the incident – your recovery order will depend on the current needs of the business at that time.	
Understanding your IT service contracts □ Check what support is included by any outsourced SAAS (Software as a Service) providers within your contract. This might include email accounts, calendars, and file storage. □ Give clear and detailed instructions what security controls you want your IT provider to implement. **For each external provider write down:** □ What data are they responsible for? □ Are back-ups included in your package? Are they turned on? □ Are there other security features you could add on or turn on?	
Be aware of exactly what is covered in your insurance policy. **If you have purchased cyber insurance:** □ Make sure the Insurer is informed at the start of the incident, as retrospective claims can be difficult. □ What service will your insurer provide in the immediate response to an incident? □ Does your insurance include IT forensic recovery? (recovering data from damaged or destroyed machines). □ Does your insurance include legal help? Or public relation support? □ Does it cover claims for compensation by third parties? (for example, if a customer's personal data is lost)	

Checklist.

Plan ahead: What could you do to protect your business?	Notes
Create a Cyber Security Incident Response Team □ Create a team who will handle the response to an incident. This step may involve input from your outsourced IT managed service provider.	
Ensure staff understand Cyber Incident Team roles □ Allocate deputies to cover for absences	
Consider what equipment may be required to run your business offline □ What would a manual process look like? □ Have a back-up communication channel e.g phone numbers, social media, intranet	
Capture business emergency contacts □ Create an emergency contact document. Include staff names and contact details, emergency contacts, customer and suppliers. □ Make a digital copy of the document available in a place you can access it easily. □ Print a hard copy of the document and keep it in a safe place. □ Consider keeping another copy of this document somewhere offsite. □ Update this document regularly (for example every 3 months)	
Share resilience plans with staff □ Train staff who feature within the incident response team on what is expected of them in their roles. □ Ensure they have a delegated deputy in case of staff absences □ Implement staff training for policies and procedures and reporting incidents	
Understand the role of social media and communications in cyber incident response. □ Create a Crisis Communication plan □ Create a Public Relations plan □ Draft responses for a variety of scenarios and timeframes, including information to get you through the first 48 hours. □ Draft content for company website – Pre-upload a draft web-page with information including FAQ and / or hotline for customers or stakeholders to call. □ Cyber and Fraud Centre's Reputational Management Framework document outlines the key steps you should take from a reputation management perspective in the event of a crisis.	

Prepare your business: Checklist

Plan ahead: What could you do to protect your business?	Notes
Make copies of your incident response plan □ Ensure you can still access your plan should computer equipment become unavailable.	
Undertake weekly IT security checks □ Undertake weekly security updates □ Regularly check you can restore your information from a back-up copy. Make sure that data is copying in a condition where it can be restored from. □ Do you need to replace or restore any technology?	
Regularly (daily / weekly) back-up computers and key documents □ Keep copies safe / offsite □ Ensure you can restore the information from it. □ https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data	
Test your Cyber Incident Response plan □ NCSC Exercise in a Box lets you test your incident response plan, ensuring staff know how to respond during an incident. It contains material for setting up, planning, delivery, and post exercise activity. □ Regularly test and check key elements of the plan □ Consider creating your own bespoke cyber exercises. This allows you to tailor these to reflect your organisation's values and threats you face.	

Checklist.

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

CyberScotland
CYBERSCOTLAND PARTNERSHIP

Cyber and Fraud Centre Scotland

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

☎ 01786 447 441
✉ enquiries@cyberfraudcentre.com
www.cyberfraudcentre.com

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27