





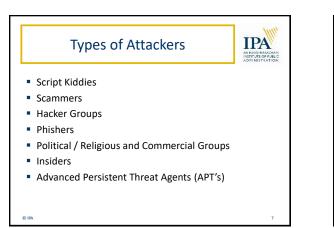
ute of Public Administration | 57-61 Lansdowne Road | Dublin 4 | Ireland | Ph. +353 1 2403600 | www.ipa.ie

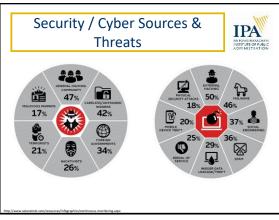
IPA IPA Introduction & Welcome Introduction to Cyber Crime INSTITUTE OF PUBL INSTITUTE OF PUBLIC Introduction to Cybercrime Cyber crime and terrorism has escalated during Where does the responsibility lie... recent years Why do we need a reponse plan It is well-organized Relevant GDPR Articles. It has advanced technically Incident Response Program Challenges It is well-financed The need for 3rd Party support 3 Phases of building Security incident response capability Cyber Incident Response Programs and Teams Cyber Breach Incident Response Checklist Preparedness Audit Checklist

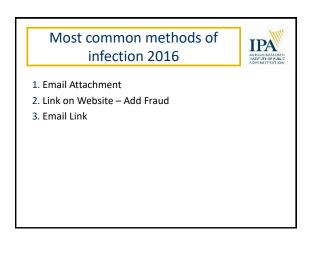




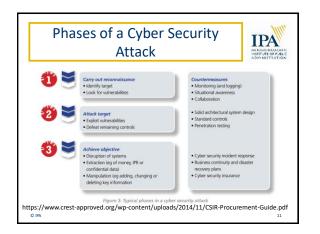


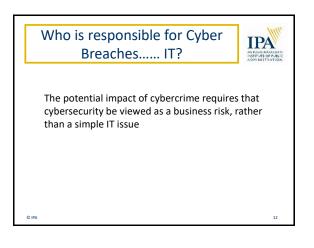




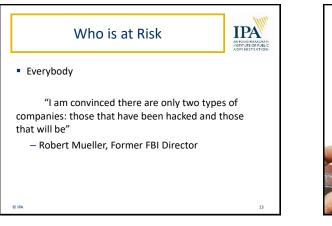












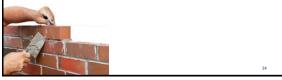


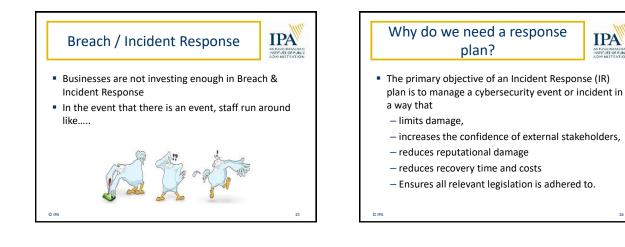


IPA

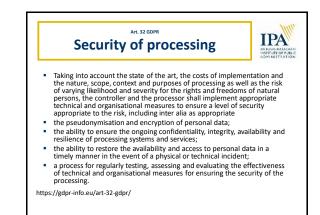
INSTITUTE OF PUBLIC

- With the current threat environment, businesses have and are increasing the priority of cybersecurity risk
- But the focus is primarily on protecting their environment from breaches.....

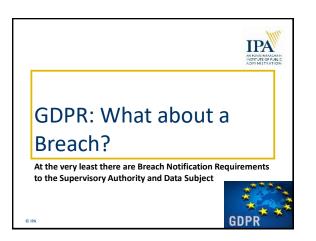








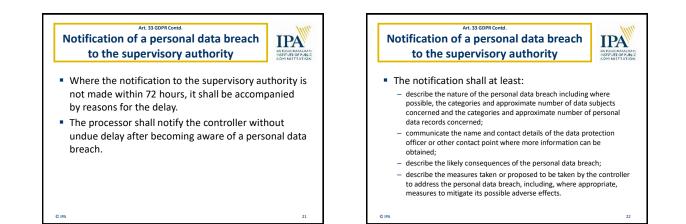




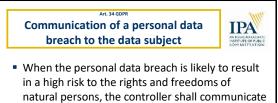
Art. 33 GDPR Contd. Notification of a personal data breach to the supervisory authority



- In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with <u>Article 55</u>, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- Contd.







- natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
 The communication shall describe in clear
- The communication shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33 (next Slide).



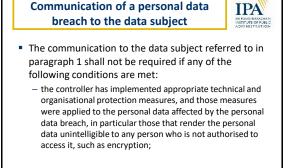
Art 33 Required Breach Notification



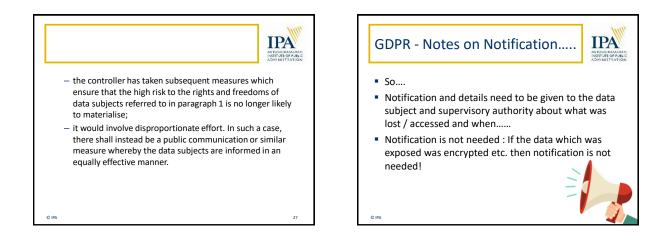
25

- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

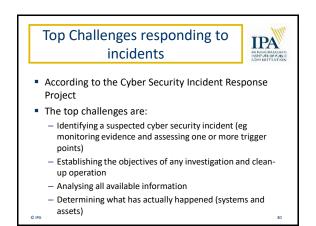
© IPA



Art. 34 GDPF

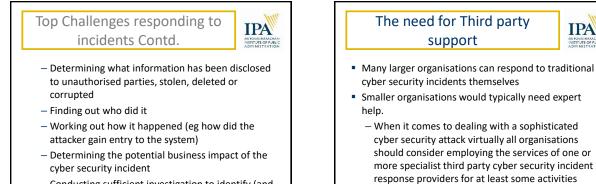








IPA



IPA

- Conducting sufficient investigation to identify (and prosecute, if appropriate) the perpetrator(s).

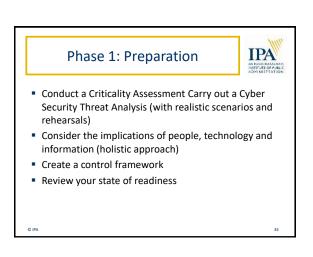
3 Phases of building

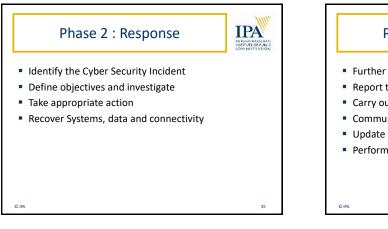
Security Incident

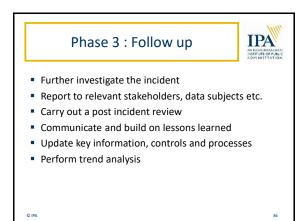
Response Capability

In order to build an effective capability, one should what

needs to be done before, during and after the attack









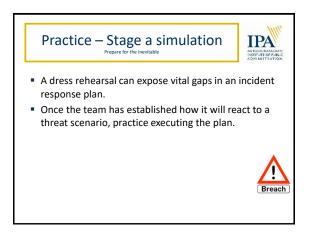


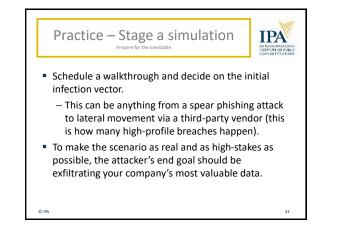


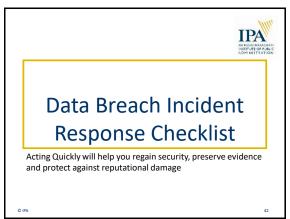




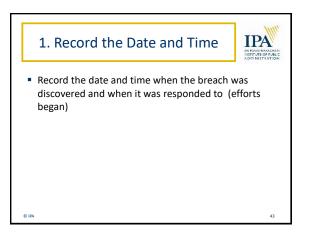
- Your team will coordinate efforts between your company's various departments and fulfil two primary functions:
 - 1. The immediate function is to develop the data breach response plan and prep the entire organization on proper protocol during a breach.
 - 2. Then, if a breach does occur, the team will implement the response plan, engage the proper resources and track the efforts.

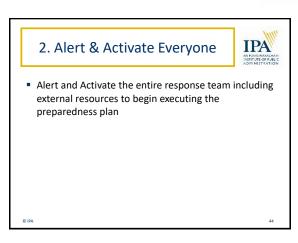


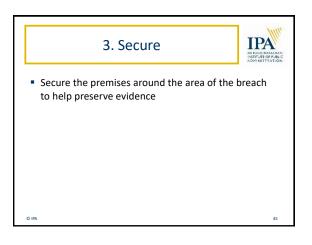


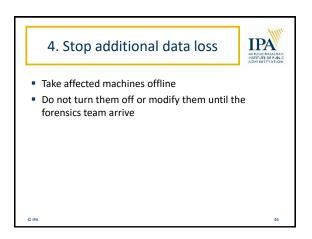


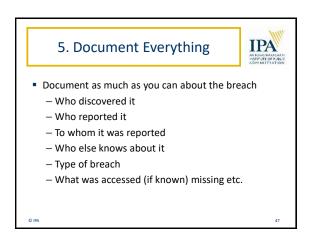






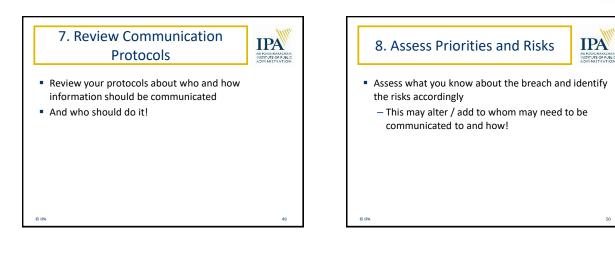


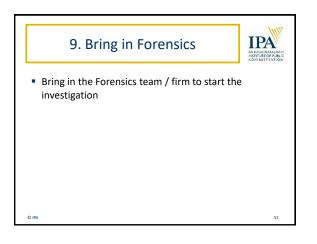


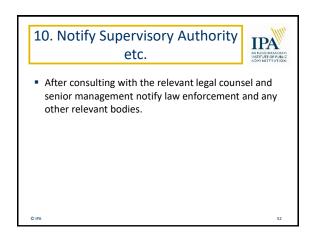


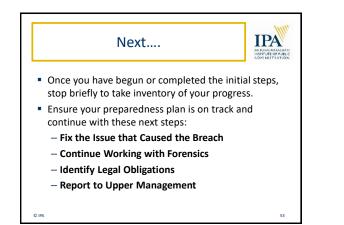


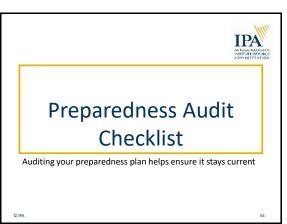














Update data breach response team contact list



- Check that contact information for internal and external members of your breach response team is current.
- Remove anyone who is no longer with your company or with an external partner and add new department heads.
- Re-distribute the updated list to the appropriate parties
 - When: Quarterly or when needed

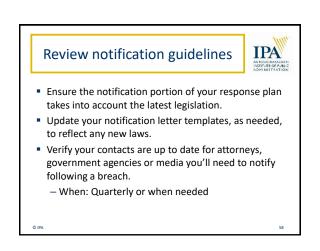
© IPA



- When: Quarterly or when needed



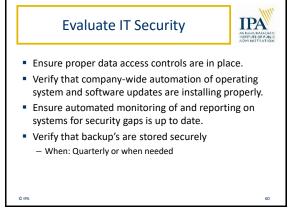
- When: Quarterly or when needed



 Check up on third parties that have access to your data
 Review how third parties are managing your data and if they are meeting your data protection standards.

- Ensure they are up to date on any new legislation that may affect you during a data breach.
- Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it.
 - When: Quarterly or when needed

0





Lastly: IPA Articles / Links of Interest IPA Review staff security awareness Ensure all staff are up to date on proper data CESG Top ten steps to cyber security First Responder's Guide - Policy and Principles from the protection procedures, including what data, centre for the protection of national infrastructure (CPNI) documents and emails to keep and what to securely GovCertUK incident response guidelines discard The Good Practice Guide for Incident Management from the Review how to spot and report the signs of a data European Network and Information Security Agency (ENISA) breach from within everyday working environments. NIST Computer Security Handling Guide (Special Publication 800-61) Verify employees are actively keeping mobile Responding to targeted cyberattacks from ISACA devices and laptops secure onsite and offsite and (collaborating with E&Y) changing passwords every three months. • Men: Ongoing 62

Software of Interest



- CAINE (Computer Aided Investigative Environment) is the Linux distro created for digital forensics. It offers an environment to integrate existing software tools as software modules in a user friendly manner. Open source. <u>http://www.caine-live.net/</u>
- SANS Investigative Forensics Toolkit SIFT is a multipurpose forensic operating system which comes with all the necessary tools used in the digital forensic process. It is built on Ubuntu with many tools related to digital forensics. free <u>http://digital-</u>
- In forensics.sans.org/community/downloads



