IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

LOCAL AUTHORITY HEADS OF INFORMATION SYSTEMS CONFERENCE 2017

Ballymascanlon Hotel, Dundalk
11-12 October 2017

Institute of
Public Administration

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

Breaches and Cyber Incident Response

Heads of IS Conference 2017

Tom Brett

CISSP, CEH CI, MCT, MCITP, CASP

Introduction & Welcome

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Introduction to Cybercrime
- Where does the responsibility lie…
- Why do we need a reponse plan
- Relevant GDPR Articles.
- Incident Response Program Challenges
- 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

Introduction to Cyber Crime

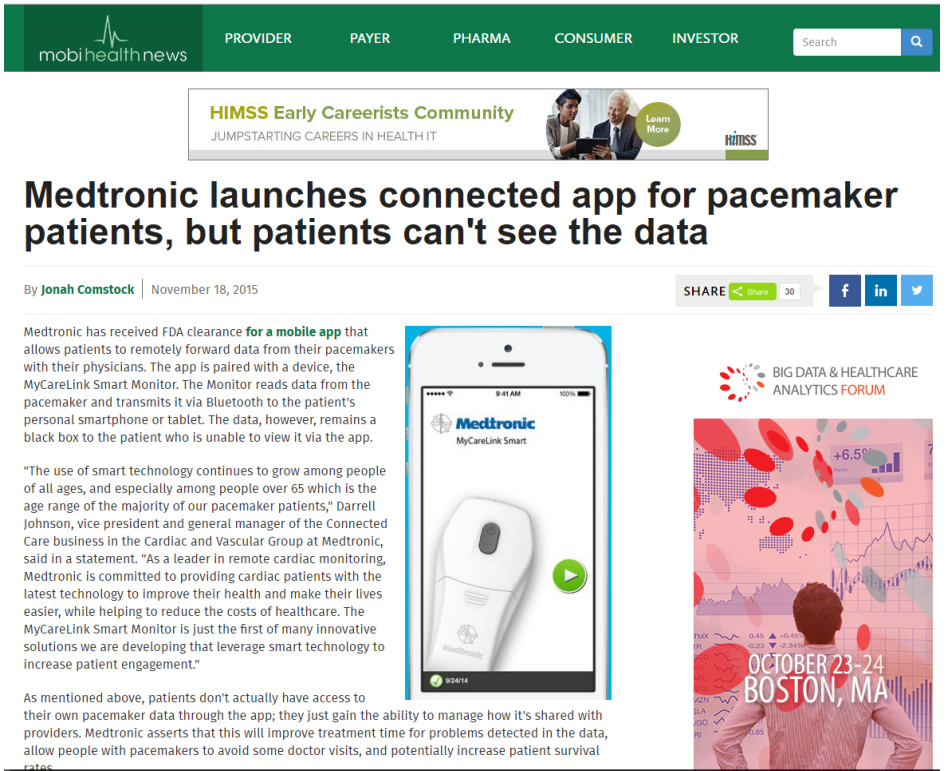
IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Cyber crime and terrorism has escalated during recent years
- It is well-organized
- It has advanced technically
- It is well-financed

The more we use the greater the problem

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC ADMINISTRATION

- The more we use IoT and technology the more we become susceptible!



mobihealthnews

PROVIDER PAYER PHARMA CONSUMER INVESTOR Search

Medtronic launches connected app for pacemaker patients, but patients can't see the data

By **Jonah Comstock** | November 18, 2015

SHARE Share 30

Medtronic has received FDA clearance **for a mobile app** that allows patients to remotely forward data from their pacemakers with their physicians. The app is paired with a device, the MyCareLink Smart Monitor. The Monitor reads data from the pacemaker and transmits it via Bluetooth to the patient's personal smartphone or tablet. The data, however, remains a black box to the patient who is unable to view it via the app.

"The use of smart technology continues to grow among people of all ages, and especially among people over 65 which is the age range of the majority of our pacemaker patients," Darrell Johnson, vice president and general manager of the Connected Care business in the Cardiac and Vascular Group at Medtronic, said in a statement. "As a leader in remote cardiac monitoring, Medtronic is committed to providing cardiac patients with the latest technology to improve their health and make their lives easier, while helping to reduce the costs of healthcare. The MyCareLink Smart Monitor is just the first of many innovative solutions we are developing that leverage smart technology to increase patient engagement."

As mentioned above, patients don't actually have access to their own pacemaker data through the app; they just gain the ability to manage how it's shared with providers. Medtronic asserts that this will improve treatment time for problems detected in the data, allow people with pacemakers to avoid some doctor visits, and potentially increase patient survival rates

Most Common Items to Protect

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Intellectual Property
- Customer's And Staff's Privacy
- Confidential Data
- System Availability
- Reputation…..

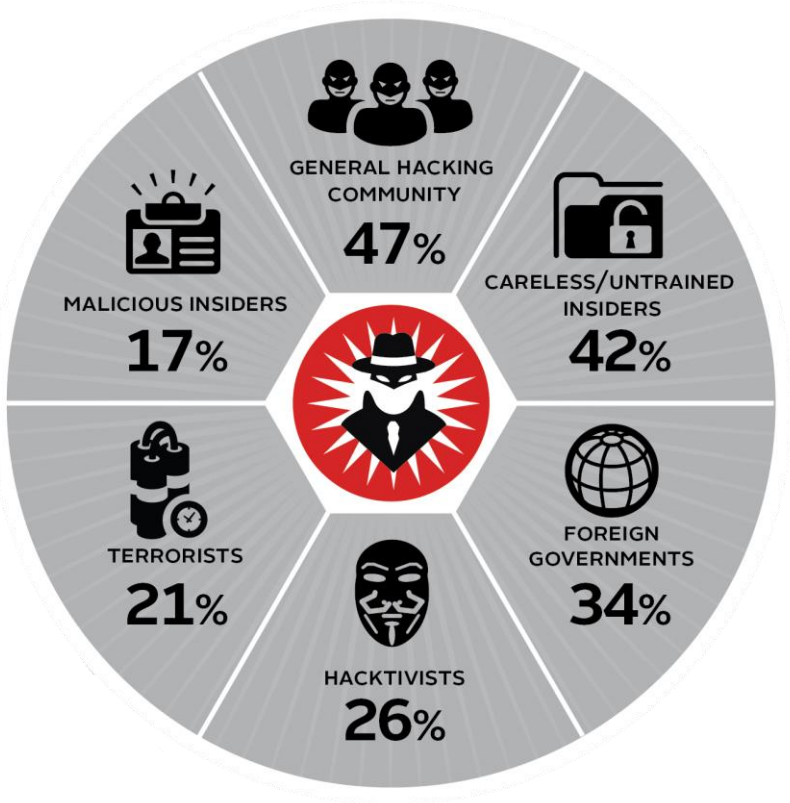
Types of Attackers

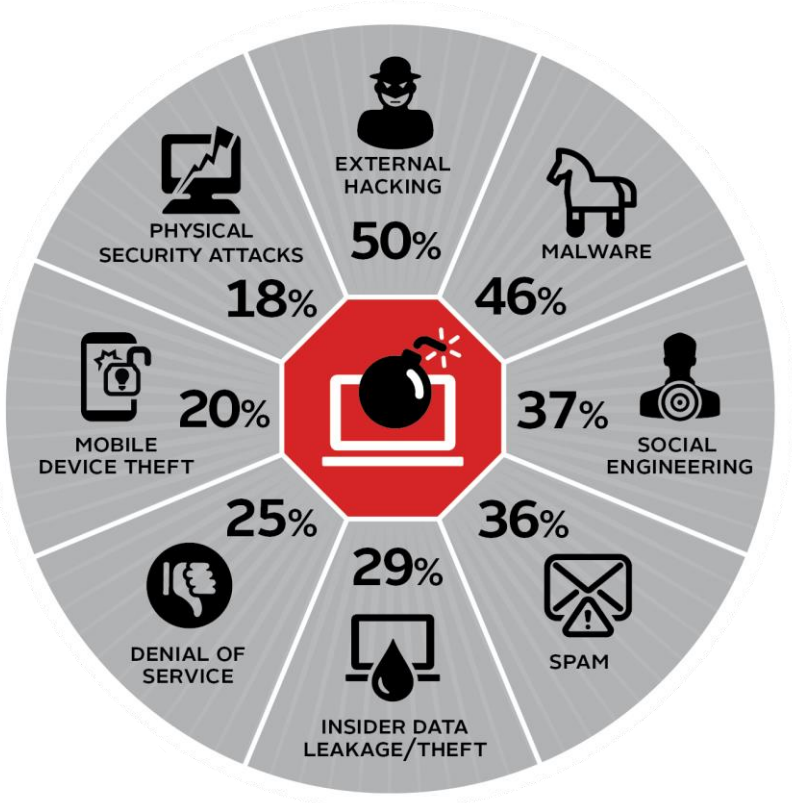
IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Script Kiddies
- Scammers
- Hacker Groups
- Phishers
- Political / Religious and Commercial Groups
- Insiders
- Advanced Persistent Threat Agents (APT's)

Security / Cyber Sources & Threats

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC ADMINISTRATION





http://www.solarwinds.com/resources/infographics/continuous-monitoring.aspx

Most common methods of infection 2016

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

1. Email Attachment
2. Link on Website – Add Fraud
3. Email Link

It is easy to fall victim
Rogue Access Point / Evil Twin

- Virgin WiFi
- ABC Free Wifi
- Faithlegg Guest Wifi
- Beaumont_Hosp_Guest_WiFI
- VodafoneWiFi
- Private-July14
- SEC
- eircom77744358
- APLECO02
- BTHub5-GHG5_5GHZ
- OnePlus3
- ABC Free WiFi
- iCO
- WCC-DATA
- WCCIT
- linksys
- sligoit
- Netgear34-5G
- NETGEAR34-5G
- eircom
- themarketbarwifi
- g-guest
- WiFi-2.4-0A52
- Dublin Airport Free-Wifi
- O2 Wifi
- BusEireann_WiFi
- SKY65FE5
- 3MobileWiFi-4F38
- TP-Link_5Ghz
- 3MobileWiFi-facb
- TP-Link_2.4Ghz
- VodafoneMobileWiFi-827743
- IT1
- AndroidHotspot4526
- FCCPublicWIFI

Phases of a Cyber Security Attack

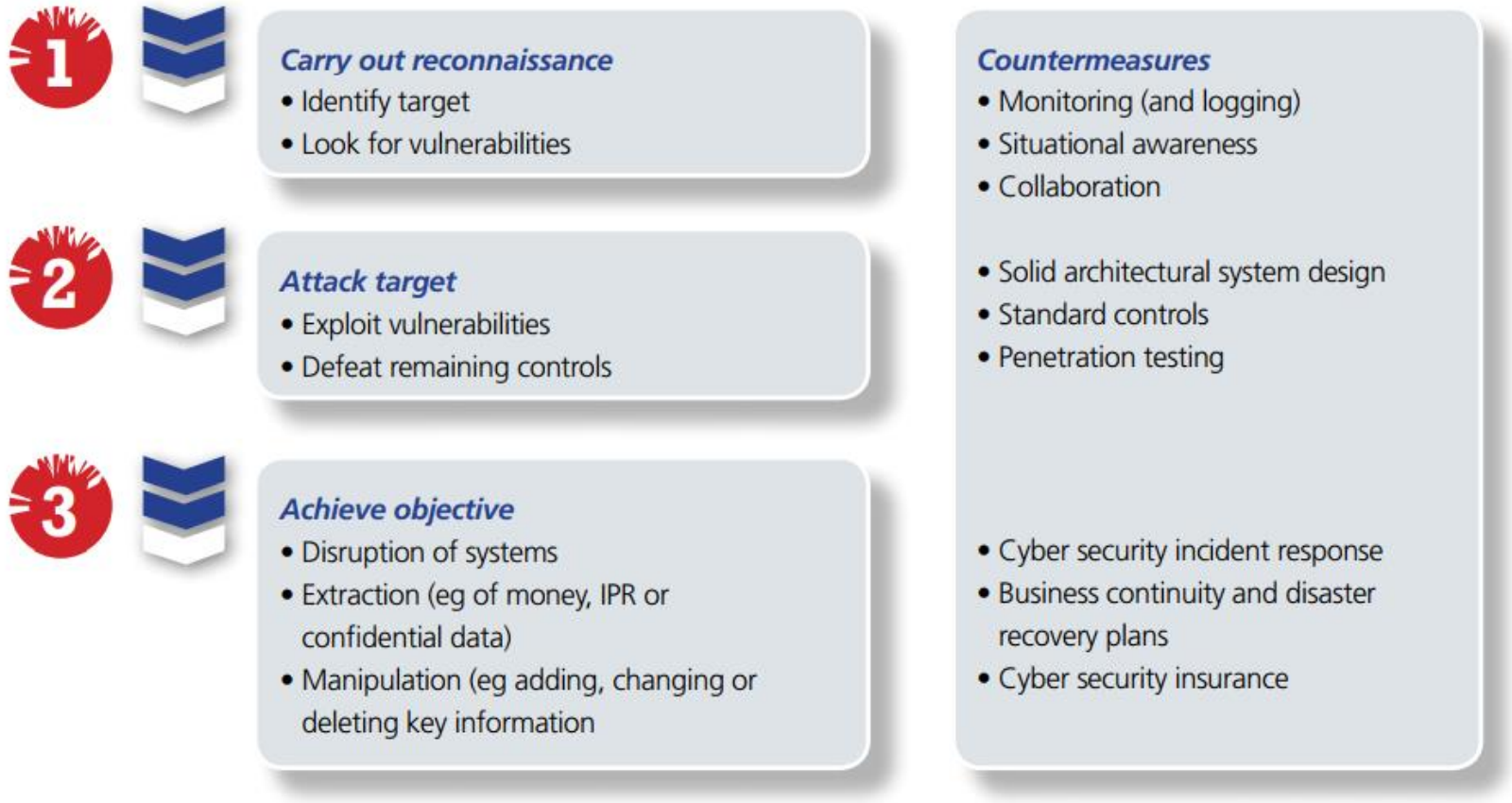


Figure 3: Typical phases in a cyber security attack

https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

Who is responsible for Cyber Breaches…… IT?

The potential impact of cybercrime requires that cybersecurity be viewed as a business risk, rather than a simple IT issue

Who is at Risk

- Everybody

"I am convinced there are only two types of companies: those that have been hacked and those that will be"

– Robert Mueller, Former FBI Director

How are businesses prepared

- 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……

Breach / Incident Response

- Businesses are not investing enough in Breach & Incident Response
- In the event that there is an event, staff run around like…..

Why do we need a response plan?

- The primary objective of an Incident Response (IR) plan is to manage a cybersecurity event or incident in a way that
  - limits damage,
  - increases the confidence of external stakeholders,
  - reduces reputational damage
  - reduces recovery time and costs
  - Ensures all relevant legislation is adhered to.

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

New GDPR Legislation….

We need to prove that adequate security measures are enforced to include testing the defences!

Art. 32 GDPR

Security of processing

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC ADMINISTRATION

- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate
- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

https://gdpr-info.eu/art-32-gdpr/

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

GDPR: What about a Breach?

At the very least there are Breach Notification Requirements to the Supervisory Authority and Data Subject

Art. 33 GDPR Contd.

Notification of a personal data breach to the supervisory authority

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC ADMINISTRATION

- 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 Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- Contd.

Art. 33 GDPR Contd.

Notification of a personal data breach to the supervisory authority

- Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Art. 33 GDPR Contd.

Notification of a personal data breach to the supervisory authority

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- The notification shall at least:
  - describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  - communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - describe the likely consequences of the personal data breach;
  - 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.

New GDPR Legislation….

Art. 34 GDPR: Communication of a personal data breach to the data subject

Art. 34 GDPR

Communication of a personal data breach to the data subject

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC ADMINISTRATION

- When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
- 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

- (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.

Art. 34 GDPR

Communication of a personal data breach to the data subject

- The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
  - the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

GDPR - Notes on Notification…..

- So….
- Notification and details need to be given to the data subject and supervisory authority about what was lost / accessed and when……
- Notification is not needed : If the data which was exposed was encrypted etc. then notification is not needed!

Incident Response Programs

Top Challenges responding to incidents

- According to the Cyber Security Incident Response Project
- The top challenges are:
  - Identifying a suspected cyber security incident (eg monitoring evidence and assessing one or more trigger points)
  - Establishing the objectives of any investigation and clean-up operation
  - Analysing all available information
  - Determining what has actually happened (systems and assets)

Top Challenges responding to incidents Contd.

- Determining what information has been disclosed to unauthorised parties, stolen, deleted or corrupted
- Finding out who did it
- Working out how it happened (eg how did the attacker gain entry to the system)
- Determining the potential business impact of the cyber security incident
- Conducting sufficient investigation to identify (and prosecute, if appropriate) the perpetrator(s).

The need for Third party support

- Many larger organisations can respond to traditional cyber security incidents themselves
- Smaller organisations would typically need expert help.
  - When it comes to dealing with a sophisticated cyber security attack virtually all organisations should consider employing the services of one or more specialist third party cyber security incident response providers for at least some activities

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

Phase 1: Preparation

- Conduct a Criticality Assessment Carry out a Cyber Security Threat Analysis (with realistic scenarios and rehearsals)
- Consider the implications of people, technology and information (holistic approach)
- Create a control framework
- Review your state of readiness

Phase 2 : Response

- Identify the Cyber Security Incident
- Define objectives and investigate
- Take appropriate action
- Recover Systems, data and connectivity

Phase 3 : Follow up

- Further investigate the incident
- Report to relevant stakeholders, data subjects etc.
- Carry out a post incident review
- Communicate and build on lessons learned
- Update key information, controls and processes
- Perform trend analysis

Cyber Breach Response Program & Team

Develop your response plan and build your response team before you need them.

Pick The Right Cyber Response Team

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Senior Management
- IT Technical Staff
- Computer Forensics Staff
- Data Protection Officer
- Public Relations Officer
- Legal Representative

Cyber Response Team Functions

- 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.

Practice – Stage a simulation

Prepare for the inevitable

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- A dress rehearsal can expose vital gaps in an incident response plan.
- Once the team has established how it will react to a threat scenario, practice executing the plan.

Practice – Stage a simulation

Prepare for the inevitable

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Schedule a walkthrough and decide on the initial infection vector.
  - This can be anything from a spear phishing attack to lateral movement via a third-party vendor (this is how many high-profile breaches happen).
- To make the scenario as real and as high-stakes as possible, the attacker's end goal should be exfiltrating your company's most valuable data.

Data Breach Incident Response Checklist

Acting Quickly will help you regain security, preserve evidence and protect against reputational damage

1. Record the Date and Time

- Record the date and time when the breach was discovered and when it was responded to (efforts began)

2. Alert & Activate Everyone

- Alert and Activate the entire response team including external resources to begin executing the preparedness plan

3. Secure

- Secure the premises around the area of the breach to help preserve evidence

4. Stop additional data loss

- Take affected machines offline
- Do not turn them off or modify them until the forensics team arrive

5. Document Everything

- Document as much as you can about the breach
  - Who discovered it
  - Who reported it
  - To whom it was reported
  - Who else knows about it
  - Type of breach
  - What was accessed (if known) missing etc.

6. Interview

- Interview all involved
- From who discovered it to everyone involved and around
- Document all

7. Review Communication Protocols

- Review your protocols about who and how information should be communicated
- And who should do it!

8. Assess Priorities and Risks

- Assess what you know about the breach and identify the risks accordingly
  - This may alter / add to whom may need to be communicated to and how!

9. Bring in Forensics

- Bring in the Forensics team / firm to start the investigation

10. Notify Supervisory Authority etc.

- After consulting with the relevant legal counsel and senior management notify law enforcement and any other relevant bodies.

Next….

- Once you have begun or completed the initial steps, stop briefly to take inventory of your progress.
- Ensure your preparedness plan is on track and continue with these next steps:
  - **Fix the Issue that Caused the Breach**
  - **Continue Working with Forensics**
  - **Identify Legal Obligations**
  - **Report to Upper Management**

Preparedness Audit Checklist

Auditing your preparedness plan helps ensure it stays current

Update data breach response team contact list

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- 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

Verify your data breach response plan is comprehensive

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies.
- Verify each response team member and department understands its role during a data breach. Create example scenarios for your response team and departments to address
  - When: Quarterly or when needed

Double check your vendor contracts

- Ensure you have valid contracts on file with your forensics firm and other vendors.
- Verify your vendors and contracts still match the scope of your business.
  - When: Quarterly or when needed

Review notification guidelines

- Ensure the notification portion of your response plan takes into account the latest legislation.
- Update your notification letter templates, as needed, to reflect any new laws.
- Verify your contacts are up to date for attorneys, government agencies or media you'll need to notify following a breach.
  - 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

Evaluate IT Security

- Ensure proper data access controls are in place.
- Verify that company-wide automation of operating system and software updates are installing properly.
- Ensure automated monitoring of and reporting on systems for security gaps is up to date.
- Verify that backup's are stored securely
  - When: Quarterly or when needed

Lastly:
Review staff security awareness

- Ensure all staff are up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard.
- Review how to spot and report the signs of a data breach from within everyday working environments.
- Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months.
  - When: Ongoing

Articles / Links of Interest

- CESG Top ten steps to cyber security
- First Responder's Guide – Policy and Principles from the centre for the protection of national infrastructure (CPNI)
- GovCertUK incident response guidelines
- The Good Practice Guide for Incident Management from the European Network and Information Security Agency (ENISA)
- NIST Computer Security Handling Guide (Special Publication 800-61)
- Responding to targeted cyberattacks from ISACA (collaborating with E&Y)

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. http://www.caine-live.net/
- **SANS Investigative Forensics Toolkit – SIFT** is a multi-purpose 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 http://digital-forensics.sans.org/community/downloads

Software of Interest

- **EnCase** is another popular multi-purpose forensic platform with tools for several areas of the digital forensic process. This tool can rapidly gather data from various devices and unearth potential evidence. Licensed. https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
- **The Sleuth Kit** is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. http://www.sleuthkit.org/

About

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

- Tom Brett
  - Senior Lecturer & Technical Advisor – Institute of Public Administration
    - Certified Ethical Hacker, Certified Chief Information Security Officer and Instructor (EC-Council),
    - Certified Information Systems Security Professional and Instructor (ISC2)
    - Numerous other Qualifications (Microsoft, Cisco, CompTIA and Academic Qualifications)
    - Working in IT for over 20 years in all aspects from Development to Systems Admin
  - ISACA Committee & Academic Co-Ordinator
  - Anti-Phishing Working Group Member (APWG)
  - tombrett@ipa.ie
  - https://ie.linkedin.com/in/thomasbrett