Cybersecurity Checklist

Data security is an ever-increasing risk for most businesses, and it seems that each week there is news of another significant data breach. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks. Many of the steps that businesses can take to limit the risk and impact of a data breach are relatively simple to implement, but require effective policies and controls to implement. Good information security crosses over a number of policies – it is not just a matter of putting in place an information security policy. The checklist below sets out the key issues that a business should deal with, and which should be implemented where appropriate across the entire suite of internal policies.

- Do you have an appropriate policy suite? A number of policies will be relevant to security:
  - Information security policy
  - Privacy policy
  - BYOD policy
  - Remote access policy
  - Network security policy
  - Acceptable use/internet access policy
  - Email and communication policy

Depending on how your policies are structured, the issues below may appear in one or more of these policies.

- Are your policies checked, updated on a regular basis, and enforced?
- Is there a board member with responsibility for cyber security?
- Does the CISO / Head of Information Security meet regularly with the board member responsible for cyber security?
- Do you have clear responsibility for cybersecurity, with clear reporting lines and decision-making authority?
- Do you ensure physical security of premises?
- Do you allocate sufficient budget to cybersecurity?
- Do you subscribe to cybersecurity updates so that you are aware of threats?
- Do you have an effective breach response plan, and do you test and update it regularly?
- Do you have appropriate cyber-liability insurance in place?

People

- Do you have appropriate mechanisms for staff to be able to report suspicious emails quickly and effectively?
- Do you train staff on cybersecurity regularly?
- Do you test staff, for example by sending spoof phishing emails?
- Do staff undertake reviews to ensure that they understand cybersecurity risks, and are results checked to ensure improvement?
- Do you have proper onboarding / off-boarding processes, and are they applied in practice?
- Do your employees understand the risks of using public WiFi?
- Do you conduct appropriate checks on new employees to understand if they are a potential security risk?

Hardware, data, encryption and technology

- Is backup data encrypted?
- Do you have appropriate mechanisms for securely sending files?
- Do you have a list of servers, and individuals who are responsible for ensuring that they are up to date?
- Do you have appropriate firewalls and intrusion detection software?
- Do you ensure that test servers are appropriately configured, and only contain dummy data?
- Are your wireless networks appropriately secured?
- Do you have email and internet traffic filtering software?
- Do you regularly check the operating systems, data and software against a 'good known state' baseline?
- Do you review unsuccessful attacks and probes / scans?
- Do you have a security roadmap, and do you review it against your overall IT roadmap regularly?
- Do you have hardware and software asset inventory lists?
- Do you have an asset management policy?
- Have you classified data by sensitivity and risk?
- Do you appropriately limit access to data?
- Do you have effective encryption of data at rest, and is encryption in transit appropriate?
- Do you back up data on a regular basis?
- Do you have an appropriate patching policy and is it applied consistently? If you use automated patching software, do you conduct periodic checks that it is operating properly?
- Do you have appropriate configuration management systems in place?
- Do you ensure that users have anti-virus software loaded and active on their devices at all times?
- Do you maintain log files for at least a year?
- Do you use automated analytics on log files?
- Do you have appropriate policies regarding use of external hard drives or USB drives?
- Do you conduct regular penetration tests and / or red teaming, with appropriate analysis of results?

Third parties

- Do you properly understand risks arising from third party service providers?
- Do you undertake appropriate due diligence before engaging third party service providers?
- Do you assess third parties for cybersecurity risk?
- Do you build appropriate contractual obligations on third parties to take steps to keep data secure?
- If you use SaaS or cloud storage, do you have appropriate contractual mechanisms to be notified quickly of potential security issues?

Remote access/BYOD

- Do you require multifactor authentication where appropriate?
- Do you allow remote access?
    - If so, do you have appropriate software and controls in place to ensure it is secure?
- Do you have appropriate policies to secure mobile devices?
    - Is data encrypted on mobile devices?
    - Can mobile devices be remotely wiped?
    - If you use BYOD, do you apply appropriate restrictions to personal use to maintain security?
    - Have you considered the use of secure areas on BYOD devices?

User accounts / passwords

- Do you require unique accounts?
- Do you require multifactor authentication where appropriate?
- Do you restrict administrator accounts to the minimum necessary?
- Do you require strong, hard to guess passwords?
- Do you automatically prevent use of common passwords?

Nothing But NET – Bringing Secure-I-T to an Insecure World.