DATA SECURITY KNOWLEDGE CHECKLIST

HIPPOGRIFF

2020 EDITION

For Investors, Business Owners, and Managers

- Has your business ever investigated the integrity of its systems?
- Is the possibility of future data breaches a top concern of management?
- Does your IT staff possess the knowledge, training, foresight, support, materials, technology, and budget to formulate a viable defense against threats?
- How are customer concerns about payment and identity theft market incidents effecting business operations?
- Have managers taken heed to the recommendations of employees in regards to implementing much needed safeguards?
- Is an internal Information Security mindset being shared with external associates?
- Are the dangers of mobile communication and portable data storage devices known by members of your organization?
- Where are sensitive electronic materials kept? How are they accessed?
- Do office visitors have proper security credentials in their possession?
- What restrictions do employees have on outside computing devices being brought into the workplace?
- Will IT equipment suppliers and distributors be held accountable for providing compromised product(s)?

- Can IT-centric personnel react fast enough and with the skills required to counter and correct compromised systems?

- Does business ownership understand the legal ramifications for not having a dedicated Cyber Security Policy in place? Are they willing to seriously consider obtaining a Managed Security Service?

- Is Cyber Security Insurance available from your current insurance provider?

- Do you handle medical or financial data? Is this data stored in-house or on third-party hosting servers?

- Are the accounts of your customers being accessed remotely or only through office workstations?

- Do you confer with competitors on the situations that they have faced?

- Should you and your department be responsible for IT matters even if you are not assigned to this area?

- The Internet of Things and Cloud Storage are two of the most dangerous technological developments that security specialists are combating; have the reasons for such dangers ever been concisely explained to you?

- Should radio controlled vehicles with wireless signal capability be allowed near business locations?

- Do you suspect digital espionage or military-grade electronic attacks are being conducted against your organization?

- Is the belief that traditional Firewall and Anti-Virus safeguards are sufficient in stopping malicious intrusions the deciding factor in IT systems deployment?

- Are regulations mandated by government and industry standards being adhered to by your organization's information infrastructure control team?

- How confident are you that your Web Developers have programmed your website to keep pace with defense against online threat vectors?

- Are you able to make the proper decisions when responding to a crisis?

- Has Hippogriff provided enough preliminary literature to proceed further?

For Technical Workers

- When was the last time you had to explain Risk, Vulnerability, and Threat differences to inquiring executive staff?
- Has the difference between Asymmetric and Symmetric encryption been a topic of discussion during relevant planning sessions? Has the difference between encryption and hashing also been elaborated on?
- How do you keep yourself updated with the information security advancements and market trends?
- What objects are being included in a thorough Penetration Testing report?
- Are Web Application Firewalls (WAFs) being maintained on a daily basis? What shortcomings has your organizations current or previous WAF been effected by?
- Are the objects of Basic Web Architecture being taken into account, and has such a fundamental been given priority consideration when planning and deploying an entirely new Webspace ecosystem or applying additional layers?
- How do you govern various security objects under your assigned scope of responsibility?
- Does a Process Audit encounter frequent disruption due to unresponsive systems or resistance from upper echelon management decisions?
- What are the differences between Policies, Processes and Guidelines within your organization?
- How are Anti-Virus alerts handled? Is there strictly an automated means of detection relied upon, or are deeper inspections of file pathways and application and operating system code being conducted through human developer review?
- Are workers who repeatedly fail to identify potentially malicious occurrences within systems being recommended to management to have their privileges revoked? Is employment termination also entertained?
- What are the main impediments to conducting day-to-day security operations?
- What are the main impediments to engaging with C-Suite to get involved with security operations and continuation?
- Is workplace experience and performance a C-Suite concern in your observation?
- Has Hippogriff provided enough preliminary literature to proceed further?

For Supporting Vendors

- Who are the key day-to-day and executive reporting contacts to be involved in case of a security incident?
- Is there a natural and cyber disaster recovery plan in place? Does it extend to clients?
- Is there a business Continuity Plan in place?
- Is there a breach notification plan in place, outlined in detail, and made available for clients to review?
- Is knowledgeable of mandated notification requirements deemed to be of a confident and competent manner by clients?
- What external plans and audits are conducted on a quarterly and annual basis if any? Do clients have access to such report results findings if legally required?
- How often are these aforementioned plans and audits updated? Have any breaches occurred? If so, when?
- Have clients been affected by internal theft of goods and materials?
- Are employees bonded, certified, licensed, etc. – who would be in contact with a client's property and data at any point of a supply chain or customer service interaction?
- How is it ensured that data is exchanged in a secure and/or private manner?
- Is verification to perform security assessments of suppliers, contractors and business partners being enforced if stipulated in commerce agreements?
- Does the client or the service provider own any exchanged data? What Terms of Service and Disclaimer provisions govern such dynamics?
- When data is "deleted," how does the deletion process ensure total removal of digital information (or even tangible papers) from a service provider's possession?
- Do clients have confirmation that qualified legal representation is retained to handle computer crime and regulatory variables?
- Have clients been forthcoming in stating all of the potential risks they may face while conducting commerce?
- Has Hippogriff provided enough preliminary literature to proceed further?

For CTOs and IT Directors

- Is your company relying on a Content Manager for its website?
- How confident are you in verifying third-party web Plug-ins and hosting integrity?
- Do you use reliable Anti-Virus/Anti-Malware software and is it updated regularly?
- Can a non-administrative user disable the anti-virus software?
- Does your Anti-Virus scan inbound and outbound email for malicious attachments? Is that function turned on?
- Are you using the default username and/or passwords for Routers or Firewalls?
- Are wireless connections authenticated with Encryption?
- Do End Users have the ability to install software on workstations and mobile systems?
- Are file sharing, games, and recreational software restricted from installation on workstations?
- Are the latest versions (or releases) of Applications used up-to-date with the latest patches?
- Are the latest versions (or releases) of Operating Systems used up-to-date latest patches?
- If legacy software is still being used, i.e. – previous versions of Microsoft Office, are Office files inspected for abnormalities?
- Is vital proprietary information (including backups) kept on Storage Devices encrypted when kept in any and all locations?
- When storage devices containing proprietary information are no longer being used are they rendered unreadable before being discarded?
- Are user accounts locked out after a specified number of unsuccessful login attempts?
- Is usage of public Instant Messaging restricted?
- Is usage of Web-based emails restricted?
- Is usage of personal Cloud accounts restricted?

- Are all workstation/server consoles locked when left unsupervised?
- Do you have a password policy covering password length, required character elements, password lifespan, and prohibitions on password sharing and saving on hard copy?
- Do passwords expire after a specified period of time, thereby requiring the user to change the password?
- Is password Reset Authority restricted to authorized persons and/or an automated password reset tool?
- Do you have an exit interview that reminds departing personnel of their responsibilities regarding protection of proprietary company information?
- Does the exit process ensure access to proprietary information is ended?
- Are background screenings of employees and contractors performed before allowing access to proprietary information?
- Do you require your third-party vendors to sign a Non-Disclosure Agreement before sharing proprietary information with them?
- Are proprietary paper documents printed/copied/faxed/stored in a secured environment and not left unsupervised when not in use?
- When no longer required, are documents shredded using a cross-cut paper shredder?
- Do you have an alarm service to detect and inform you or the authorities, if there is an unauthorized physical access to your office during non-business hours?
- How often are you conducting behavioral profiling on workers and visitors in and around operational locations, if at all?
- Has a Threat Model been formulated for each and every department within your organization?
- Has Hippogriff provided enough preliminary literature to proceed further?

U.S. Toll Free: 1-866.273.4831 | Email: inquiry@hippogriff.tech

Disclaimer: Answers to this Checklist are to be used internally; not to be utilized with external associations. Answers to listed questions are not to be documented, shared, or stored outside of the prescribed Chain of Custody agreed upon by the user of this Checklist and authorized parties.