2017 Edition. Subject to change.

Enterprise Data Security Policy Checklist

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 form a 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 components 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 distributers 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 3rd party offsite 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?

- Did you know that The Internet of Things and Cloud Storage are two of the most dangerous developments that Cyber Security specialists are facing?

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

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

- 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?

Cyber Security Statistics Sampling

- Percentage of U.S. adults that suffered some kind of security incident between Dec. 1st, 2015 and Dec. 1st, 2016: 51%

- Global spending on information security products and services in 2016: $81.6bn

- Number of reported data breaches in 2015: 781

- Fiscal year 2015 estimated global cost of Cyber Attacks annually: $400bn

- Projected global cost of Cyber Attacks in 2019: $2.1 Trillion

- Average total cost of a data breach (Global) in fiscal year 2015: $3.8mn

- Average total cost of a data breach (U.S.) in 1st quarter 2016: $6.5mn

- Percentage -- as of first quarter 2016 -- that the cost of data breaches increased from 2013-2015: 23%

- Estimated average cost incurred per stolen record in a data breach as of 2nd quarter 2015: $154 per Record

- Average annual amount of Cyber Security incidents as of 2nd quarter 2015: 80-90 Million

- Increase in Cyber Security incidents from 2014-2015 as of 3rd quarter 2015: 38%

- Top means of Cyber Attack in as of 4th quarter 2015: Phishing and Malware

- Percentage of phishing messages that were opened by the receiver in 2015: 30%

- Percentage of people that opened a phishing message in 2015 that also clicked on the malicious attachment or link: 12%

- Number of cyber security job openings as of 2nd quarter 2016: 1 Million

- Percentage of IT departments that store privileged and/or admin passwords in a Word document or spreadsheet on a company PC or laptop as of 3rd quarter 2016: 40%

- More than half of organizations hit with exploits in 2016 containing Ransomware Payloads: 67%

- Increase in social media Phishing scams rose in 2016: 500%

- Number of disclosed vulnerabilities in 2016 reaches all time high: 15,000
- Identity fraud hit U.S. victims in 2016: 15.5 Million
- Amount of IT professional that don't know how to improve security posture: 50%
- Records exposed in data breaches in 2016: 4.2 Billion
- Percent of organizations that have technical challenges protecting data: 93%
- Data breach disclosure 2016 jump: 40%
- Fraud for online holiday sales spike in 2016: 31%
- 2016 minimum successful Ransomware theft: 1 Billion
- Percent of businesses experiencing data loss due to employee turnover: 69%
- Percent of consumers who would respond to a retailer breach by switching to cash: 55%
- Healthcare major Cyber Attack 2016 growth increase: 63%
- Number of companies that currently miss reporting data breaches: 44%
- DDoS attack year-on-year increase: 40%
- Estimated Cyber Insurance market top by 2022: $14 Billion
- Consumer users that were knowingly compromised in the last 12 months - 51%
- Percent of Ransomware attacks that successfully bypassed email filtering over in the past 12 months: 77%
- Antivirus failure rate -- while the only countermeasure tool available -- to stop Ransomware: 100%
- Forecasted Card-Not-Present (CNP) fraud increase by 2020: 2.1 Billion
- IT decision makers admitting they don't have a any Cyber Security strategy in place: 50%
- Global Cyber Security industry forecasted worth by 2020: 2.2 Trillion
- Has Hippogriff provided enough preliminary literature to proceed further?

For CTOs & IT Directors

- Is your company relying on a Content Manager for its website?
- How confident are you in verifying 3rd 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/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 key proprietary information (including backups) kept on Storage Devices/Materials encrypted when stored 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 3rd parties 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: 1-866.273.2436 | Email: inquiry@hippogriff.tech

Disclaimer: This Checklist is to be used internally. It is 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 the provider, Hippogriff GmbH & Ltd. © 2015-2017 | All rights are reserved.