BISC

Business Internet Safety Checklist

Michael Nuccitelli, Psy.D.
www.ipredator.co

Business Internet Safety Checklist (BISC)

The Business Internet Safety Checklist (BISC) is a 100-item checklist designed for a business to verify, upgrade or monitor their internet safety and cyber security practices. The BISC is a data collection tool that investigates a business's vulnerability of being targeted, disparaged, slandered, stolen from or infiltrated by cybercriminals, disgruntled past employees, angry customers or nefarious corporate competitors.

Related to cybercrime specific areas, the BISC focuses the business on their cyber security breach potential, digital reputation acumen and ability to institute internet safety and cyber security strategies. With the rapid growth and expansion of Information and Communications Technology (ICT), all businesses now must distribute a part of their operating budget to both cyber security and digital reputation management.

It is recommended to complete the BISC on a quarterly basis if corporate competitors or internal employee sabotage are suspected of engaging in online disparagement and internet defamation to the online reputation or brand[s] of the business. The BISC also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

BISC DIRECTIONS

1. The time needed to complete the BISC checklists averages 60-90 minutes.

2. To complete the checklist, you must respond to each statement with 1 of 4 choices as follows:

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

3. Only answer "Yes" or "No" to statements you are positive about or almost certain.

4. If there is a question you do not understand, respond with choice D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

5. If there is a question that does not apply to you or the subject being queried, respond with choice D. DNA__ (Does Not Apply, Not Applicable, Not Relevant). For example, if a checklist statement addresses mobile devices, but you do not own a mobile device, you would respond with choice DNA__.

6. Please provide a response to each question with 1 of the 4 responses before calculating your final score. All questions have been designed to make scoring easy to compile. Simply add up your correct responses (+1) along with (+1) for your D. DNA__ responses and compare your score to the scoring key including in this file.

7. Prior to taking the checklist, please review the following two definitions and refer to them if needed. The definition of Information and Communications Technology (ICT) and iPredator are as follows:

ICT: Information and Communications Technology (ICT) is an umbrella term used to define any electronic or digital communication device or application used to obtain, exchange or disseminate information. ICT stresses the role of unified communications and the integration of telecommunications, which enable users to create access, store, transmit and manipulate information.

ICT consists of all forms of telecommunication, information technology, broadcast media, audio and video processing, transmission and network-based control and monitoring functions. Information and Communications Technology (ICT) is a concept incorporating all electronic and digital forms of communication.

iPredator: A child, adult, group or nation who, directly or indirectly, engages in exploitation, victimization, stalking, theft or disparagement of others using Information and Communications Technology (ICT.) iPredators are driven by deviant fantasies, desires for power and control, retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance or personal and financial gain. iPredators can be any age, either gender and not bound by economic status, race or national heritage.

iPredator is a global term used to distinguish anyone who engages in criminal, deviant or abusive behaviors using Information and Communications Technology (ICT.) Whether the offender is a cyberbully, cyberstalker, cyber harasser, cybercriminal, online sexual predator, internet troll, online child pornography consumer or cyber terrorist, they fall within the scope of iPredator. The three criteria used to define an iPredator include:

I. A self-awareness of causing harm to others, directly or indirectly, using ICT.
II. The intermittent to frequent usage of Information and Communications Technology (ICT) to obtain, exchange and deliver harmful information.
III. A general understanding of Cyberstealth used to engage in criminal or deviant activities or to profile, identify, locate, stalk and engage a target.

Unlike human predators prior to the Information Age, iPredators rely on the multitude of benefits offered by Information and Communications Technology (ICT.) These assistances include exchange of information over long distances, rapidity of information exchanged and the infinite access to data available. Malevolent in intent, iPredators rely on their ability to deceive others using Information and Communications Technology (ICT) in an abstract electronic universe.

"*All my checklists and inventories are designed to assess the subject's internet safety acumen, cyber-attack awareness, cyber security practices and general understanding of knowing how to protect oneself in today's digital device environment. Scoring well does not need the respondent to be an advanced information technology professional. If anything, being advanced in electronic devices can give some a false sense of security. Few people score 95% and higher on their first attempt as we are all living at the beginning of a new paradigm called, the Information Age".* Michael Nuccitelli Psy.D., iPredator Inc.

BISC

Business Internet Safety Checklist

Note: The term "business" in the BISC stands for any of the following: owner(s), employees, business consultants or the business itself as an entity.

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

1. The business is ICT safe from hackers and checked regularly for updates.
2. The business is ICT safe from viruses and checked regularly for updates.
3. The business is ICT safe from malware and checked regularly for updates.
4. The business is ICT safe from a mobile device cyber-security breach and checked regularly for updates.
5. The business has a formal written internet security policy.
6. The business engages in internet safety training.
7. The business's ICT get automatic software and security updates.
8. The business knows what is needed to prevent a security breach of sensitive information.
9. The business protects sensitive company data on mobile devices.
10. The business monitors how employees interact with social media.
11. The business checks for new cybercrime protection products and services.
12. The business monitors sensitive online information and knows the value to a cybercriminal.
13. The business knows the consequences of using the internet in an unsafe manner.
14. The business tracks social networking sites employees visit during downtime at the job location.
15. The business is educated on safe online practices.
16. The business diversifies the company ICT passwords.
17. The business knows how to combat the latest cyber threats.
18. The business is safe from a loss of financial data.
19. The business is safe from customer and financial information theft.
20. The business is safe from loss of employee data.
21. The business has guidelines on how long to keep online documents.
22. The business has social media guidelines on what is permissible to share online.
23. The business knows how to safeguard private, personal and financial information.
24. The business educates consultants and employees on cyber security and cyber-attack solutions.
25. The business has a customized cyber security plan.
26. The business has passwords that are complex and not easily guessable.
27. The business understands the importance of not showing financial information online.
28. The business limits and tailors' access to ICT to reduce the risk of an internal breach.
29. The business has a plan for cyber-attacks and what to do in case of a network breach.

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

30. The business knows how to report hacking, stolen finances or identities.
31. The business has a formal social media policy for employees that are reviewed regularly.
32. The business has an Internet usage policy clarifying what websites and web service employees can use.
33. The business checks social media comments about the business.
34. The business has a plan if there is a loss of customer and employee information.
35. The business informs partners/suppliers how you protect their information.
36. The business knows cybercriminals target businesses with poor online safety protection.
37. The business keeps up with new mobile and social media platforms.
38. The business has guidelines for employees' use of social media.
39. The business is prepared for *"Social Engineering"* attacks.
40. The business keeps up with news on mobile device security vulnerabilities.
41. The business uses *"Multifactor Authentication"* to access networks.
42. The business completely wipes data from ICT devices before disposing them.
43. The business forbids the use of USB devices in the workplace.
44. The business has an effective digital defense plan in the event of a digital reputation crisis.
45. The business has an online corporate statement in case of a digital reputation crisis.
46. The business has a press release in case of a digital reputation crisis.
47. The business has a video message in the event of a digital reputation crisis.
48. The business has a social media mention in case of a digital reputation crisis.
49. The business has a formal e-mail statement in the event of a digital reputation crisis.
50. The business has a Tweet in case of a digital reputation crisis.
51. The business has a micro-site or dark site that can be activated in the event of a digital reputation crisis.
52. The business knows delaying a response to business complaints allows criticism to spread virally.
53. The business knows the longer business criticism goes unanswered, the more truthful it appears and the more defensive a response seems.
54. The business knows inaccurate rumors left unchallenged online can be highly problematic.
55. The business is proficient at getting out the facts effectively in the event of a digital reputation attack.
56. The business is aware that a disgruntled customer or ex-employee can cause havoc with the business reputation.
57. The business knows that prompt and effective action is critical to protecting the digital reputation.
58. The business encrypts the hard drives to help protect vital data in case of theft or loss.

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

59. The business uses pass codes for mobile phones and subscribed to a remote wipe service.
60. The business knows what personal information is stored in files and all internet enabled devices.
61. The business monitors who sends sensitive personal information from the business.
62. The business monitors how personal and financial information is issued online.
63. The business knows what kind of information is collected at each entry point.
64. The business knows where collected information at each entry point is kept (i.e., central computer database, individual laptops, disks, cloud).
65. The business monitors how personally identifying information (i.e., social security numbers, credit card numbers, financial information) is stored.
66. The business shreds and destroys customer credit card information unless it has a business need.
67. The business checks the default settings of the software that reads customer credit card numbers and processes transactions.
68. The business has a written records retention policy to identify what information must be kept and how it is secured.
69. The business only uses social security numbers for required and lawful purposes.
70. The business refrains from using social security numbers as employee or customer identification numbers.
71. The business has a data security plan that includes physical & electronic security, employee training and the security practices of contractors and service providers.
72. The business identifies the computers or servers where sensitive personal information is stored.
73. The business identifies all connections to the computers where sensitive information is stored.
74. The business assesses the vulnerability of its social media profiles to cyber-attacks.
75. The business refrains from storing sensitive customer data on internet enabled devices with an internet connection unless it is essential.
76. The business checks their security software vendors' websites regularly for alerts about new vulnerabilities.
77. The business scans all internet enabled devices on the network to identify and profile the operating system and open network services.
78. The business receives and transmits sensitive financial data using a Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.
79. The business uses password activated screen savers to lock employee computers after a period of inactivity.
80. The business locks out users who do not enter their correct password within a designated number of log-on attempts.

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

81. The business at once changes vendor-supplied default passwords in a more secure strong password when installing new software.
82. The business restricts the use of laptops to those employees who do not need them to perform their jobs.
83. The business requires employees to store laptops in a secure place.
84. The business requires employees to immediately notify someone if there is a potential security breach.
85. The business investigates security incidents at once and takes steps to close off existing threats to personal information.
86. The business password protects all mobile devices that hold sensitive data and encrypts them.
87. The business knows how to securely back up all the mobile devices often.
88. The business habitually keeps an eye on all portable electronic devices.
89. The business turns off wireless services when they are not being used.
90. The business knows exactly who and what are connected always.
91. The business keeps mobile device security software current by having the latest mobile security software, web browsers and operating systems.
92. The business knows what data (i.e., location, access to the social networks) on mobile devices an application can access before it is downloaded.
93. The business knows how to disable the geotagging feature on mobile phones.
94. The business knows about Wi-Fi hotspots and what types of business functions to limit.
95. The business knows when banking and/or shopping using mobile devices to look for web addresses with "https://" or "shttp://".
96. The business is educated about and protected from credit card fraud.
97. The business is educated about and protected from identity theft.
98. The business is educated about DHL/UPS scams.
99. The business is educated about Escrow Services Fraud.
100. The business is educated about Internet Extortion.

Yes Answers___ No Answers___ I Do Not Know___ Does Not Apply___

Yes Answers___ + Does Not Apply___ = BISC Score___

CORRECT RESPONSE TO ALL STATEMENTS: Y__ (Yes, Agree, True)

Note: The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. "I Do Not Know" & "No" responses should be addressed at once with a plan of action. Although obtaining a score of 90 or higher indicates a minimal probability of a successful cyber-attack, it is still crucial to be alert and prepared to defend against iPredators, ex-partners and those who would seek to destroy your digital reputation. As information and communications technology continues to expand, it will become increasingly important to manage and watch cyber-attack prevention and digital reputation.

(link for web page scoring key)

Internet Safety Tool Scoring Keys Page: https://www.ipredator.co/scoring-keys/

Given the rapid expansion and advancements in ICT, it is recommended to complete the BISC on a quarterly basis and more often if an iPredator is suspected of engaging in a possible cyber-attack. To achieve optimal cybercrime, cyber-attack and/or cyber assault prevention, the goal is to score in the upper 10%-15% of all the IISC assessments. Although cyberspace is a non-physical abstract electronic universe, the toll it can take on vulnerable and/or ignorant ICT users can be very real and can range from frustrating to deadly.

IISC SCORE DEFINITION

IISC Score: Upon completion of any of the IISC assessments, the respondent will have a final score ranging from 0-75, 0-100 or 0-300 depending on the IISC assessment. In this formula, the score represents the risk potential and vulnerability of the ICT user, the business or the subject being queried from being targeted by a cyberbully, cyberstalker, cybercriminal, nefarious corporate competitor or online sexual predator. Whether taken one time or on multiple occasions, the goal is to finish with a score in the top 10% of all the IISC assessments.

IISC SCORING KEY

Business Internet Safety Checklist
BISC

Note: It is recommended that the business conduct this checklist on a quarterly basis. The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. "IDK". Wrong responses should be addressed at once with a report to superiors of a plan of action. As Information and Communications Technology continues to expand, it will become increasingly important to manage and monitor cyber-attack prevention and corporate digital reputation.

Score: (1-10)
Category: Guaranteed Corporate Target and Extremely Vulnerable.
Risk Potential: Alarmingly High.
Present and/or Future iPredator Involvement: Certain.
Intervention Plan: Professional Consultation Highly Advised.
Level of Urgency: Urgent Attention Required.

Score: (11-29)
Category: Prime Corporate Target and Extremely Vulnerable.
Risk Potential: High.
Present and/or Future iPredator Involvement: Almost Certain.
Intervention Plan: Professional Consultation Highly Advised.
Level of Urgency: Immediate Attention Required.

Score: (30-39)
Category: Probable Corporate Target and Extremely Vulnerable.
Risk Potential: Moderately High.
Present and/or Future iPredator Involvement: Involvement Likely.
Intervention Plan: Professional Consultation Highly Advised.
Level of Urgency: Immediate Attention Strongly Recommended.

Score: (40-55)
Category: Likely Corporate Target and Moderate Vulnerability.
Risk Potential: Moderate.
Present and/or Future iPredator Involvement: Involvement Suspected.
Intervention Plan: Create and Implement an iPredator Prevention Plan.
Level of Urgency: Immediate Attention Recommended.

Score: (56-78)
Category: Possible Corporate Target and Moderate Vulnerability.
Risk Potential: Moderate.
Present and/or Future iPredator Involvement: Involvement Possible.
Intervention Plan: Increase iPredator Protection & Prevention Strategies.
Level of Urgency: Immediate Attention Suggested.

Score: (79-89)
Category: Skilled ICT Protection and Low Vulnerability.
Risk Potential: Mild.
Present and/or Future iPredator Involvement: Possible, but Unlikely.
Intervention Plan: Continue iPredator Protection & Prevention Strategies.
Level of Urgency: Not Urgent, Important to Address if Score Below 85.

Score: (90-100)
Category: Advanced ICT Protection and Minimal Vulnerability.
Risk Potential: Minimal.
Present and/or Future iPredator Involvement: Unlikely.
Intervention & Education Plan: Consider Educating Others.
Level of Urgency: 0%, All iPredator Issues Addressed.

Michael Nuccitelli, Psy.D.

Michael Nuccitelli, Psy.D. is a NYS licensed psychologist, cyberpsychology researcher and online safety educator. In 2009, Dr. Nuccitelli finalized his dark side of cyberspace concept called iPredator. Since 2010, he has advised those seeking information about cyberbullying, cyberstalking, cybercriminal minds, internet addiction and his Dark Psychology concept. By day Dr. Nuccitelli is a practicing psychologist, clinical supervisor and owner of MN Psychological Services, PLLC. After work and on the weekends, he volunteers helping online users who have been cyber-attacked. Dr. Nuccitelli's is always available to interested partied and the media at no cost. The iPredator website and everything created by Dr. Nuccitelli is educational, free and public domain.