Employee Security Awareness Survey

Trenton Bond
trent.bond@gmail.com
Admin - Version 1.3

Security Awareness

One of the most significant security risks that organizations and corporations face today is not with systems or applications but with employees. A study of about 700 IT security practitioners released this year (2012) by the Ponemon Institute finds that "over 78 percent of respondents say negligent or malicious employees or other insiders have been responsible for at least one data breach within their organizations over the past two years" [Trendmicro, 2012, "The Human Factor in Data Protection"]. Historically, businesses and organizations have primarily focused on lowering the risk associated with technical solutions. However, little, if any, resources have been allocated to improving the weak security posture of employees.

An important and critical initiative to mitigate this growing risk is a security awareness program. Most programs include training for employees regarding the organization's security policies, standards for handling sensitive data, email best practices, how to report a potential breach, and general security principles that, if followed, will help protect the individual and the corporation. Similar to the importance of measuring and tracking the strength of system defenses, it is equally important to measure the effectiveness of an awareness program and the strength of employee defenses.

Security Awareness Survey

A great tool to measure the effectiveness and strength of the organization's security awareness program is with a survey. This "Employee Security Awareness Survey" has been designed to ask employees how they would respond to specific security related questions and situations. The results of this survey can be used to determine areas of the program that need to be improved and to calculate a risk score, or the probability of compromise or breach involving employees. The generated score and risk level can be tracked over time as a metric to measure program goals and initiatives, or it can also be used to compare with industry peers.

Using this Survey to Determine Risk

This survey consists of 25 questions. Some of the question responses in this survey indicate strong awareness and good security practices while others indicate weak awareness, negligent behavior, or high-risk activities. Based on these differences, each question response in this survey (except for the first question) has been assigned a risk value (1-5). "One" is the lowest risk value and "five" is the highest risk value. When the results of the survey have been collected, they can be used to determine the overall risk score or risk level of the organization.

1. For each of the 25 questions, multiply each question response risk value (1-5) by the number of times it was chosen by the survey takers.

   <response risk value> X <the number of times chosen> = <response total>

2. Add up all of the response totals for a survey cumulative response total.
3. Divide the survey cumulative response total by the number of survey takers to calculate the survey (or organization's) risk score.

   <cumulative response total> / <number of survey takers> = Organization's Risk Score

4. Using the risk score, check the "Risk Levels" table below for the organization's general risk rating.

Risk Levels

Risk Levels	Description
Low (25 – 39)	Users are aware of good security principles and threats, have been properly trained, and comply with all organizational security standards and policies.
Elevated (40 – 60)	Users have already been trained on organizational security standards and policies, they are aware of threats, but may not follow good security principles and controls.
Moderate (61 – 81)	Users are aware of threats and know they should follow good security principles and controls, but need training on organizational security standards and policies. They also may not know how to identify or report a security event.
Significant (82 – 96)	Users are not aware of good security principles or threats nor are they aware of or compliant with organizational security standards and policies.
High (97 – 110)	Users are not aware of threats and disregard known security standards and policies or do not comply. They engage in activities or practices that are easily attacked and exploited.

Survey Minimum Risk Score = 25
Survey Maximum Risk Score = 110

Ideas on how to Deploy this Survey

Below are some ideas and elements to consider when deploying this survey.

1. Identify survey stakeholders such as the IT Department, Security Division, HR, etc. and an executive level sponsor such the CEO, CIO, or CISO.
2. Have the survey reviewed and approved by public relations, HR, or legal.
3. Identify the scope of users you want to take the survey (employees, contractors, volunteers, etc.)
4. Determine if the survey will be required or is voluntary. If it is voluntary, what is the motivation or is there a prize for taking the survey?
5. Evaluate and chose a survey engine or learning management system from which to conduct to the survey (Google, Survey Monkey, etc.).
6. Determine how long to leave the survey open.
7. Deliver results and risk score to stakeholders and executive sponsorship for review.
8. Track the risk score over time in a graph to measure the organization's improvement.
9. Consider sharing and comparing the organization's risk score with other organizations or businesses of similar size and industry.
10. The wording of the questions can be changed to fit your environment or situation as long as the responses remain the same. This will allow for flexibility in the survey but maintain some consistency in the risk score when tracked over time or compared with others.

1. What is your position within the company?
    a. Full time employee
    b. Part time employee
    c. Contractor
    d. Partner
    e. Vendor
    f. Other

Logic Note: Did not apply risk values to positions because they should all be equally security aware.

2. Do we have a security team?
    a. Yes, we have a company security team. (1)
    b. No, we do not have a company security team. (4)
    c. I do not know. (3)

    Logic Note: Users who chose "C" are not informed and pose a risk for obvious reasons. Users who choose "B" when there really is a security team could represent an even higher risk to the organization because they believe they are aware but are really misinformed.

3. Do you know who to contact in case you are hacked or if your computer is infected?
    a. Yes, I know who to contact. (1)
    b. No, I do not know who to contact. (5)

    Logic Note: Users who do not know who to contact when their PC is compromised pose a significant risk because they are likely to continue to use the device, potentially exposing the organization to further compromise or breach.

4. Have you ever found a virus or Trojan on your computer at work?
    a. Yes, my computer has been infected before. (4)
    b. No, my computer has never been infected. (2)
    c. I do not know what a virus or Trojan is. (4)

    Logic Note: Users who are unaware of malware threat pose a significant risk to an organization and would likely not know how or when to report it.

    Users who indicate they are aware of malware threat but still have had infected work computers also pose a significant risk. Their activities and/or behaviors, while at work, may have led to the infections (sites they visit, links they click, etc.). However, the risk is slightly lowered because users who have been infected in the past are usually more security aware.

5. Do you know how to tell if your computer is hacked or infected?
    a. Yes, I know what to look for to see if my computer is hacked or infected. (1)
    b. No, I do not know what to look for to see if my computer is hacked or infected. (4)

    Logic Note: Users who do not know what potential symptoms to look for are more likely to continue to use a compromised device, potentially exposing the organization to further compromise or breach.

6. Have you ever given your password from work to someone else?
    a. Yes (5)
    b. No (1)

    Logic Note: Users who are willing to share their work password are highly susceptible to social engineering or internal threats. The easiest way to get a password is to ask.

7. If you format a hard drive or erase the files on it all the information on it is permanently lost.
    a. True (4)
    b. False (1)

    Logic Note: Users who choose "A" could represent a significant risk to the organization because they believe they are aware but are really misinformed and likely do not dispose of sensitive electronic documents properly.

8. How secure do you feel your computer is?
    a. Very secure (3)

b. Secure (1)
c. Not secure (4)

Logic Note: Users who feel their computer is not very secure may be right and the issue should be escalated to the responsible party. However, the user may be less likely to handle sensitive data or conduct risky transactions with it, which would lower the impact of compromise slightly.

Users who feel their computer is very secure may be right and so the device poses little vulnerability risk to the organizations. However, the user may be more likely to handle sensitive data or conduct risky transactions with it, which would increase the impact of compromise.

Cautious but aware users who chose "Secure" seemed like a good middle ground to strive for.

9. Is the firewall on your computer enabled?
   a. Yes, it is enabled. (1)
   b. No, it is not enabled. (5)
   c. I do not know what a firewall is. (4)

Logic Note: Users who chose "C" are not informed and pose a significant risk for obvious reasons. Users who choose "B" are even a higher risk as they know what a firewall is and the protection it would provide; yet do not have it enabled.

10. Is your computer configured to be automatically updated?
    a. Yes, it is. (1)
    b. No, it is not. (5)
    c. I do not know. (3)

Logic Note: Users who chose "C" are not informed and pose a risk for obvious reasons. Users who choose "B" are even a higher risk as they know what "automatic updates" means and the protection it would provide; yet do not have it configured.

11. How careful are you when you open an attachment in email?
    a. I always make sure it is from a person I know and I am expecting the email. (1)
    b. As long as I know the person or company that sent me the attachment I open it. (3)
    c. There is nothing wrong with opening attachments. (5)

Logic Note: Users who choose "B" could be tricked into opening malicious attachments from spoofed sources that look like they came from recognizable persons or companies.

Users who choose "C" pose a significant risk to the organization because they are unaware of the threat, vulnerability or impact if they open a malicious attachment.

Cautious and aware users will choose "a".

12. Do you know what a phishing attack is?
    a. Yes, I do. (1)
    b. No, I do not. (5)

Logic Note: Users who are aware of how to identify phishing are less likely to fall victim lowering risk.

13. Do you know what an email scam is and how to identify one?
    a. Yes I do. (1)
    b. No, I do not. (5)

Logic Note: Users who are aware of how to identify an email scam are less likely to fall victim lowering risk.

14. Is anti-virus currently installed, updated and enabled on your computer?
    a. Yes it is. (1)
    b. No it is not. (5)
    c. I do not know how to tell. (4)
    d. I do not know what anti-virus is. (5)

Logic Note: Users who choose "B" may be indicative of users who are aware of what "anti-virus" is and the protection it provides, yet do not run or update it. This behavior may also indicate the user is risk tolerant and is more likely to improperly handle sensitive data or conduct risk transactions.

Users who choose "C" pose a significant risk because they are aware of what "anti-virus" is, but unaware of how to tell whether or not it is running.

Users who choose "D" pose a high risk because they are unaware of what "anti-virus" is and unaware of how to tell whether or not it is running.

15. My computer has no value to hackers, they do not target me.
    a. True (5)
    b. False (1)

Logic Note: Users who choose "A" pose a significant risk to the organization because they are unaware of the threat and impact if their computer is compromised.

16. Do we have policies on which websites you can visit?
    a. No, there are no policies, I can visit whatever websites I want while at work. (4)
    b. Yes, there are policies limiting what websites I can and cannot visit while at work, but I do not know the policies. (2)
    c. Yes, there are policies and I know and understand them. (1)

Logic Note: Users who choose "B" are protected by corporate filtering solutions, but are an elevated risk because they are unaware of the policies.

Users who choose "A" pose a significant risk because they can visit whatever site they want including potentially malicious sites.

17. Do we have policies on how what you can and cannot use email for?
    a. No, there are no policies, I can send whatever emails I want to whomever I want while at work. (4)
    b. Yes, there are policies limiting what emails I can and cannot send while at work, but I do not know the policies. (2)
    c. Yes, there are policies and I know and understand them. (1)

Logic Note: Users who choose "B" are protected by corporate filtering solutions, but are an elevated risk because they are unaware of the policies.

Users who choose "A" pose a significant risk because they can visit whatever site they want including potentially malicious sites.

18. Is instant messaging allowed in our organization?
    a. Yes, instant messaging is allowed in our organization. (1)
    b. No, instant messaging is not allowed in our organization. (1)
    c. I do not know. (2)

Logic Note: Users who choose “A” or “B” are indicative of uses that are aware of organizational policy regardless of disposition. Users who choose “C” are not aware of or perhaps a policy does not exist elevating the risk.

19. Can you use your own personal devices, such as your mobile phone, to store or transfer confidential company information?
    a. Yes I can. (5)
    b. No I cannot. (1)
    c. I do not know. (4)
    d. Yes I can, if using the company provided solution. (2)

Logic Note: Users who choose “A” represent a high risk to the organization because there is little if any control over the processing, transmitting, or storing of sensitive data on personal devices.

Users who choose “C” pose a significant risk because at minimum they are unaware of whether or not it is allowed, and they are more likely to handle confidential information on personal devices without knowing.

20. Have you downloaded and installed software on your computer at work?
    a. Yes I have. (2)
    b. No I have not. (1)

Logic Note: Users who choose “A” pose a higher risk to the organization than those who choose “B” because they are more likely to download malicious software and infect a work computer.

21. Has your boss or anyone else you know at work asked you for your password?
    a. Yes, they have (4)
    b. No, they have not. (1)

Logic Note: Organizations where it is common and accepted for others to ask users for their passwords is more likely to be successfully attacked with social engineering.

22. Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?
    a. Yes I do. (4)
    b. No I do not. (1)

Logic Note: When third party accounts are compromised, users who use the same password on work as personal accounts are much more vulnerable to password attacks and guessing.

23. How often do you take information from the office and use your computer at home to work on it?
    a. Almost every day. (5)
    b. At least once a week. (4)
    c. At least once a month. (2)
    d. Never (1)

Logic Note: Users who answer “A”, B”, or “C” pose an increasing risk of data loss to organizations based on increasing frequency and the use of a home personal computer.

24. Have you logged into work accounts using public computers, such as from a library, cyber café or hotel lobby?
    a. Yes, I have (4)
    b. No, I have not (1)

Logic Note: Users who access work accounts from public computers are more likely to have their credentials or corporate data stolen if these devices are insecure or compromised. This would also indicate the user is not aware of the potential risks of doing so.

25. If you delete a file from your computer or USB stick, that information can no longer be recovered.
    a. True (4)
    b. False (1)

Logic Note: Users who choose "A" could represent a significant risk to the organization because they believe they are aware but are really misinformed and likely do not dispose of sensitive electronic documents properly.