transfer mode (ATM) network, a virtual private network (VPN), or any combination of any of the same. Communications links 202 and 205 may be any communications links suitable for communicating between workstations 201 and server 204, such as network links, dial-up links, wireless links, hard-wired links, and the like. ~~etc.~~ Connectivity may also be supported to a CCTV or image/iris capturing device.

[38] With some embodiments, illustrative system 200 may support an interactive system as will be further discussed. For example, workstations 201 may function as user terminals and server 204 may function as a security application control system that monitors activities of multiple user accounts on workstations 201. As understood by those skilled in the art, the steps that follow in FIGS. 3-6 may be implemented by one or more of the components in FIG. 1 and 2 and/or other components, including other computing devices.

[39] Aspects of the invention relate to monitoring, measuring, or detecting activities relating to one or more controls. The controls may relate to disparate activities associated with user accounts. Monitoring controls may assist further determinations whether a user account represents a threat to an organization. In one embodiment, one or more of the "user accounts" may be associated with a particular individual, such as an employee of an organization. Thus, regardless of whether the individual is using user terminal 141, user terminal 151, or any workstation 201, the individual's actions may be tied to a particular user account. In an alternative embodiment, a "user account" may be associated with a particular computing device. Thus, in one embodiment, if any of a plurality of individuals uses a particular computing device, such as user terminal 141, the computing device will be a specific user account. In another embodiment, a "user account" may be a combination of specific user(s) on specific computing device(s).

[40] As would be understood by those skilled in the art, it is quite common for a subset of user accounts within an organization or domain to have access to resources not available to other user accounts within the same organization or domain. Unlike prior art systems, embodiments disclosed herein may be used to monitor activities across an organization or domain having user accounts with security features that differ from other user accounts. For example, in one embodiment, each user account may have access to a first network, such as the "Internet" through WAN 131 shown in FIG. 1, however, only a subset of those accounts may have access to a second network, such as

We claim:

1. A computer-readable medium comprising computer-executable instructions that when executed by a processor cause the processor to perform:

detecting activities associated with a plurality of user accounts involving a plurality of control groups;

determining that a threshold quantity of activities violated at least two controls in the control groups comprising:

detecting that a user account accessed a first storage device;

determining if the user account has permission rights to conduct the access to the first storage device;

wherein if the user account does not have permission rights to conduct the access, determining that an activity violation has occurred, wherein if the user account does have permission rights to conduct the access, determining that an authorized access occurred and storing an attribute value of the access;

determining that at least one activity violation has occurred; and

calculating a predictive threat rating for the first user account.

2. The computer-readable medium of claim 1, further comprising instructions that when executed by the processor cause the processor to perform:

determining whether an indicator is associated with the first user account, wherein the additional indicator is selected from the group consisting of: a prior investigation of a user of the user account, a prior investigation of another individual, the volume or type of information accessible by the user account, whether the user account has an exception to a security policy, and combinations thereof.

3. The computer-readable medium of claim 1, wherein the control groups comprise controls selected from the group consisting of: removable media controls, unencrypted transmission controls, encrypted targeted communication controls, and combinations thereof.

4. The computer-readable medium of claim 1, further comprising instructions that when executed by the processor cause the processor to perform:

receiving an indication that a first attribute value of an unblocked targeted communication from a first user account is similar to a first attribute value of a blocked transmission from the first user account.

5. The computer-readable medium of claim 1, wherein an attribute of the access is selected from the group consisting of: a filename accessed, a size of a file accessed, a location of a file accessed, metadata regarding a file accessed, or combinations thereof.

6. The computer-readable medium of claim 5, wherein the computer-readable medium is operatively detachable from the processor.

7. The computer-readable medium of claim 6, further comprising instructions that when executed by the processor cause the processor to perform:

detecting the presence of a removable computer-readable medium; and

comparing a value identifying the removable computer-readable medium against a collection of identifiers.

8. The computer-readable medium of claim 4, further comprising instructions that when executed by the processor cause the processor to perform:

comparing one or more attribute values against criteria to determine if an activity violation occurred.

9. The computer-readable medium of claim 4, further comprising instructions that when executed by the processor cause the processor to perform:

quantifying a quantity of attribute values of authorized accesses during a first time period; and

determining if an activity violation occurred.

10. The computer-readable medium of claim 4, wherein the blocked transmission comprises a targeted communication and the first attribute relates to criteria selected from the group consisting of: encryption status, attachment, recipient of a targeted communication, patterns, words, and combinations thereof.

11. An apparatus comprising:

a processor;

a control module configured to detecting activities associated with a plurality of user accounts in regards to a plurality of controls;

a computer-readable medium comprising computer-executable instructions that when executed by the processor cause the apparatus to perform:

determining that a threshold quantity of activities violated at least two controls in the control groups comprising:

detecting that a user account accessed a first storage device;

determining if the user account has permission rights to conduct the access to the first storage device;

wherein if the user account does not have permission rights to conduct the access, determining that an activity violation has occurred, wherein if the user account does have permission rights to conduct the access, determining that an authorized access occurred and storing an attribute value of the access;

determining that at least one activity violation has occurred; and

calculating a predictive threat rating for the first user account.

12. The apparatus of claim 11, wherein the controls are selected from the groups consisting of: removable media controls, unencrypted transmission controls, encrypted targeted communication controls, and combinations thereof.

13. The apparatus of claim 11, wherein the controls consist essentially of: removable media controls, unencrypted transmission controls, encrypted targeted communication controls, and combinations thereof.

14. The apparatus of claim 11, wherein an attribute value of the access relates to an attribute selected from the group consisting of: a filename accessed, a size of a file accessed, a location of a file accessed, metadata regarding a file accessed, or combinations thereof.

15. The apparatus of claim 11, the instructions further comprising:

detecting the presence of a removable computer-readable medium; and

comparing a value identifying the removable computer-readable medium against a collection of identifiers.

16. The apparatus of claim 11, the instructions further comprising:

comparing one or more attribute values against criteria to determine if an activity violation occurred.

17. The apparatus of claim 11, the instructions further comprising:

quantifying a quantity of attribute values of authorized accesses during a first time period; and

determining if an activity violation occurred.

18. The apparatus of claim 11, the instructions further comprising:

receiving an indication that a first attribute value of an unblocked targeted communication from a first user account is similar to a first attribute value of a blocked transmission from the first user account;

wherein the blocked transmission comprises a targeted communication and the first attribute of the blocked transmission relates to criteria selected from the group consisting of: encryption status, attachment, recipient of a targeted communication, patterns, words, and combinations thereof.

19. A computer-readable medium comprising computer-executable instructions that when executed by a processor cause the processor to perform:

detecting activities associated with a plurality of user accounts in regards to a plurality of control groups, wherein at least one of the control groups comprises a plurality of targeted communication controls;

determining that a threshold quantity of activities violated at least two controls in the control groups comprising:

detecting that a user account accessed a first storage device;

determining if the user account has permission rights to conduct the access to the first storage device;

wherein if the user account does not have permission rights to conduct the access, determining that an activity violation has occurred, wherein if the user account does have permission rights to conduct the access, determining that an authorized access occurred and storing an attribute value of the access;

determining that at least one activity violation has occurred; and

calculating a predictive threat rating for the first user account.

20. The computer-readable medium of claim 19, wherein an attribute value of the authorized access relates to an attribute selected from the group consisting of: a filename accessed, a size of a file accessed, a location of a file accessed, metadata regarding a file accessed, and combinations thereof.

We claim:

1. A non-transitory computer-readable medium comprising computer-executable instructions that when executed by a processor cause the processor to perform:

detecting activities associated with a plurality of user accounts within a business entity and involving a plurality of control groups, wherein each user account is associated with a different individual of the business entity, wherein the plurality of user accounts comprises a first user account and a second user account, and wherein at least one of the control groups comprises a plurality of targeted communication controls;

for at least the first and the second user accounts, determining that a threshold quantity of activities violated at least two controls in the control groups comprising:

detecting that the first and the second user account accessed a first storage device;

determining that the first user account does not have permission rights to conduct the access to the first storage device, and in response, determining that an activity violation for a first control of the at least two controls has occurred and storing an attribute value of the violation;

determining that the second user account does have permission rights to conduct the access, and in response, determining that an authorized access occurred and storing an attribute value of the access; and

responsive to determining that the threshold quantity of activities violated the at least two controls in the control groups, and responsive to determining that an activity violation has occurred, calculating a predictive threat rating for the first user account using the stored attribute value of the violation.

2. The computer-readable medium of claim 1, further comprising instructions that when executed by the processor cause the processor to perform:

determining whether an indicator is associated with the first user account, wherein the additional indicator is selected from the group consisting of: a prior investigation of a user of the user account, a prior investigation of another individual, the volume or type of information accessible by the user account, whether the user account has an exception to a security policy, and combinations thereof.

3. The computer-readable medium of claim 1, wherein the control groups comprise controls selected from the group consisting of: removable media controls, unencrypted transmission controls, encrypted targeted communication controls, and combinations thereof.

4. The computer-readable medium of claim 1, further comprising instructions that when executed by the processor cause the processor to perform:

receiving an indication that a first attribute value of an unblocked targeted communication from a first user account is similar to a first attribute value of a blocked transmission from the first user account.

5. The computer-readable medium of claim 4, further comprising instructions that when executed by the processor cause the processor to perform:

comparing one or more attribute values against criteria to determine if an activity violation occurred.

6. The computer-readable medium of claim 4, further comprising instructions that when executed by the processor cause the processor to perform:

quantifying a quantity of attribute values of authorized accesses during a first time period; and

determining if an activity violation occurred.

7. The computer-readable medium of claim 4, wherein the blocked transmission comprises a targeted communication and the first attribute relates to criteria selected from the group consisting of: encryption status, attachment, recipient of a targeted communication, patterns, words, and combinations thereof.

8. The computer-readable medium of claim 1, wherein an attribute of the access is selected from the group consisting of: a filename accessed, a size of a file accessed, a location of a file accessed, metadata regarding a file accessed, or combinations thereof.

9. The computer-readable medium of claim 8, wherein the computer-readable medium is operatively detachable from the processor.

10. The computer-readable medium of claim 9, further comprising instructions that when executed by the processor cause the processor to perform:

detecting the presence of a removable computer-readable medium; and

comparing a value identifying the removable computer-readable medium against a collection of identifiers.

11. An apparatus comprising:

a processor;

a control module configured to detect activities associated with a plurality of user accounts in regards to a plurality of controls in a plurality of control groups, wherein each user account is associated with a different individual of a business entity, wherein the plurality of user accounts comprises a first user account and a second user account and wherein at least one of the control groups comprises a plurality of targeted communication controls;

a non-transitory computer-readable medium comprising computer-executable instructions that when executed by the processor cause the apparatus to perform:

determining that a threshold quantity of activities violated at least two controls in the control groups comprising:

detecting that a user account accessed a first storage device;

determining if the user account has permission rights to conduct the access to the first storage device;

wherein if the user account does not have permission rights to conduct the access, determining that an activity violation has occurred, wherein if the user account does have permission rights to conduct the access, determining that an authorized access occurred and storing an attribute value of the access;

determining that at least one activity violation has occurred; and

responsive to determining that the threshold quantity of activities violated at the least two controls in the control groups, and responsive to determining that at least one activity violation has occurred, calculating a predictive threat rating for the first user account.

12. The apparatus of claim 11, wherein the controls are selected from the groups consisting of: removable media controls, unencrypted transmission controls, encrypted targeted communication controls, and combinations thereof.

13. The apparatus of claim 11, wherein the controls consist essentially of: removable media controls, unencrypted transmission controls, encrypted targeted communication controls, and combinations thereof.

14. The apparatus of claim 11, wherein an attribute value of the access relates to an attribute selected from the group consisting of: a filename accessed, a size of a file accessed, a location of a file accessed, metadata regarding a file accessed, or combinations thereof.

15. The apparatus of claim 11, the instructions further comprising:

detecting the presence of a removable computer-readable medium; and

comparing a value identifying the removable computer-readable medium against a collection of identifiers.

16. The apparatus of claim 11, the instructions further comprising:

comparing one or more attribute values against criteria to determine if an activity violation occurred.

17. The apparatus of claim 11, the instructions further comprising:

quantifying a quantity of attribute values of authorized accesses during a first time period; and

determining if an activity violation occurred.

18. The apparatus of claim 11, the instructions further comprising:

receiving an indication that a first attribute value of an unblocked targeted communication from a first user account is similar to a first attribute value of a blocked transmission from the first user account;

wherein the blocked transmission comprises a targeted communication and the first attribute of the blocked transmission relates to criteria selected from the group consisting of:

encryption status, attachment, recipient of a targeted communication, patterns, words, and combinations thereof.

19. A non-transitory computer-readable medium comprising computer-executable instructions that when executed by a processor cause the processor to perform:

detecting activities associated with a plurality of user accounts in regards to a plurality of control groups, wherein at least one of the control groups comprises a plurality of targeted communication controls;

determining that a threshold quantity of activities violated at least two controls in the control groups comprising:

detecting that a user account accessed a first storage device;

determining if the user account has permission rights to conduct the access to the first storage device;

wherein if the user account does not have permission rights to conduct the access, determining that an activity violation has occurred, wherein if the user account does have permission rights to conduct the access, determining that an authorized access occurred and storing an attribute value of the access;

determining that at least one activity violation has occurred; and

responsive to determining that the threshold quantity of activities violated at the least two controls in the control groups, and responsive to determining that at least one activity violation has occurred, calculating a predictive threat rating for the first user account.

20. The computer-readable medium of claim 19, wherein an attribute value of the authorized access relates to an attribute selected from the group consisting of: a filename accessed, a size of a file accessed, a location of a file accessed, metadata regarding a file accessed, and combinations thereof.