Abstract: Methods, computer-readable media, software, and apparatuses may monitor consumer information in order to determine a probability of a data breach associated with a customer based on an online presence of the customer. The probability of a data breach may be used to present metrics to a consumer and/or a service provider. Further, the consumer may be presented with information indicating what factors contribute to the probability of a data breach, as well as information regarding how to reduce those factors.

[Continued on next page]

Published:
— with international search report (Art. 21(3))
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))
CYBER-SECURITY PRESENCE MONITORING AND ASSESSMENT

CROSS-REFERENCE TO RELATED APPLICATIONS


FIELD OF ART

[02] Aspects of the disclosure generally relate to methods and computer systems, including one or more computers particularly configured and/or executing computer software. More specifically, aspects of this disclosure relate to systems for capturing, evaluating, and communicating cyber-security data.

BACKGROUND

[03] People and organizations may collect and/or analyze information, such as personal or confidential information of a user. Further, services, such as credit monitoring services or identity protection services, may monitor a user's account in order to determine if a data breach has occurred. As consumers continue to gain an ever-increasing presence in online environments, there will be an ever-present need to better protect consumers from confidential information being breached (e.g., made available publicly) in order to protect consumers from fraud and/or other harms.

BRIEF SUMMARY

[04] In light of the foregoing background, the following presents a simplified summary of the present disclosure in order to provide a basic understanding of some aspects of the invention. This summary is not an extensive overview of the invention. It is not intended to identify key or critical elements of the invention or to delineate the scope
of the invention. The following summary merely presents some concepts of the invention in a simplified form as a prelude to the more detailed description provided below.

[05] Aspects of the disclosure address one or more of the issues mentioned above by disclosing methods, computer readable storage media, software, systems, and apparatuses for providing information relating to a risk of a data breach associated with a consumer. This may promote awareness regarding the risk of a data breach involving the consumer.

[06] Aspects of this disclosure provide a cyber-security data processing system that may identify a consumer, monitor for the presence of confidential information associated with the consumer, and/or establish a value associated with the cyber-security risks associated with the consumer. The cyber-security data processing system may collect information from various networks, devices, and/or services. The cyber-security data processing system may then calculate a value based on a probability that the consumer may experience a data breach. In some instances, the information and/or value may be presented on a marketplace for consumption by service providers.

[07] Of course, the methods and systems of the above-referenced embodiments may also include other additional elements, steps, computer-executable instructions, or computer-readable data structures. In this regard, other embodiments are disclosed and claimed herein as well. The details of these and other embodiments of the present invention are set forth in the accompanying drawings and the description below. Other features and advantages of the invention will be apparent from the description, drawings, and claims.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[08] The present invention is illustrated by way of example and is not limited by the accompanying figures in which like reference numerals indicate similar elements and in which:
FIG. 1 illustrates an example security monitoring device or environment that may be used in accordance with one or more aspects described herein.

FIG. 2 illustrates an example system architecture for gathering and analyzing cybersecurity data in accordance with one or more aspects described herein.

FIG. 3 illustrates an example system for collecting information from various information data sources to determine an online presence for a consumer in accordance with one or more aspects described herein.

FIG. 4 illustrates an example user interface displaying an example rating screen in accordance with one or more aspects described herein.

FIG. 5 illustrates an example training quiz in accordance with one or more aspects described herein.

FIG. 6 illustrates an example breakdown screen for a component in accordance with one or more aspects described herein.

FIG. 7 illustrates an example method for determining a value associated with a potential for data breach of a consumer's data in accordance with one or more aspects described herein.

DETAILED DESCRIPTION

In accordance with various aspects of the disclosure, methods, computer-readable media, software, and apparatuses are disclosed for protecting consumers against data breaches. A consumer may be presented with a wide range of consumer risks, including cyber-extortion (e.g., ransomware), false/fraudulent account creation, credit card theft, credit score reduction, banking theft, and tax fraud. By monitoring and notifying a user of the potential for (or the occurrence of) data breaches, a system can diagnose vectors for data breaches, prevent future breaches, and/or provide recovery options if a breach occurs.
In the following description of the various embodiments of the disclosure, reference is made to the accompanying drawings, which form a part hereof, and in which is shown by way of illustration, various embodiments in which the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made.

In one or more arrangements, aspects of the present disclosure may be implemented with a computing device. FIG. 1 illustrates a block diagram of an example security monitoring device 100 that may be used in accordance with aspects described herein. The security monitoring device 100 may be a computing device, such as a personal computer (e.g., a desktop computer), server, laptop computer, notebook, tablet, smartphone, vehicles, home management devices, home security devices, smart appliances, etc. The security monitoring device 100 may have a data collection module 101 for retrieving and/or analyzing data as described herein. The data collection module 101 may be implemented with one or more processors and one or more storage units (e.g., databases, RAM, ROM, and other computer-readable media), one or more application specific integrated circuits (ASICs), and/or other hardware components (e.g., resistors, capacitors, power sources, switches, multiplexers, transistors, inverters, etc.). Throughout this disclosure, the data collection module 101 may refer to the software and/or hardware used to implement the data collection module 101. In cases where the data collection module 101 includes one or more processors, such processors may be specially configured to perform the processes disclosed herein. Additionally, or alternatively, the data collection module 101 may include one or more processors configured to execute computer-executable instructions, which may be stored on a storage medium, to perform the processes disclosed herein. In some examples, the security monitoring device 100 may include one or more processors 103 in addition to, or instead of, the data collection module 101. The processor(s) 103 may be configured to operate in conjunction with data collection module 101. Both the data collection module 101 and the processor(s) 103 may be capable of controlling operations of the security monitoring device 100 and its associated components, including RAM 105, ROM 107, an input/output (I/O) module
109, a network interface 111, and memory 113. For example, the data collection module 101 and processor(s) 103 may each be configured to read/write computer-executable instructions and other values from/to the RAM 105, ROM 107, and memory 113.

The I/O module 109 may be configured to be connected to an input device 115, such as a microphone, keypad, keyboard, touchscreen, and/or stylus through which a user of the security monitoring device 100 may provide input data. The I/O module 109 may also be configured to be connected to a display device 117, such as a monitor, television, touchscreen, etc., and may include a graphics card. The display device 117 and input device 115 are shown as separate elements from the security monitoring device 100; however, they may be within the same structure. On some security monitoring devices 100, the input device 115 may be operated by users to interact with the data collection module 101, including providing user information and/or preferences, device information, account information, warning/suggestion messages, etc., as described in further detail below. System administrators may use the input device 115 to make updates to the data collection module 101, such as software updates. Meanwhile, the display device 117 may assist the system administrators and users to confirm/appreciate their inputs.

The memory 113 may be any computer-readable medium for storing computer-executable instructions (e.g., software). The instructions stored within memory 113 may enable the security monitoring device 100 to perform various functions. For example, memory 113 may store software used by the security monitoring device 100, such as an operating system 119 and application programs 121, and may include an associated database 123.

The network interface 111 allows the security monitoring device 100 to connect to and communicate with a network 130. The network 130 may be any type of network, including a local area network (LAN) and/or a wide area network (WAN), such as the Internet, a cellular network, or satellite network. Through the network 130, the security monitoring device 100 may communicate with one or more other computing
devices 140, such as laptops, notebooks, smartphones, tablets, personal computers, servers, vehicles, home management devices, home security devices, smart appliances, etc. The computing devices 140 may also be configured in a similar manner as security monitoring device 100. In some embodiments the security monitoring device 100 may be connected to the computing devices 140 to form a "cloud" computing environment.

[22] The network interface 111 may connect to the network 130 via communication lines, such as coaxial cable, fiber optic cable, etc., or wirelessly using a cellular backhaul or a wireless standard, such as IEEE 802.11, IEEE 802.15, IEEE 802.16, etc. In some embodiments, the network interface may include a modem. Further, the network interface 111 may use various protocols, including TCP/IP, Ethernet, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), etc., to communicate with other computing devices 140.

[23] The methods and software for capturing and communicating vehicle telematics data as disclosed herein may be implemented on one or more security monitoring devices 100 used in various network environments.

[24] FIG. 2 illustrates a block diagram illustrating system architecture 200 for gathering and analyzing cyber-security data. The cyber-security data processing system (CSDPS) 202, which may also be referred to as the processing system 202 and/or the central processing system 202, may collect information from and transmit information to a consumer through various different channels such as a user mobile computing device 210, a user computing device 208, a password manager 206, banking application 218, and a web application 224. In some instances, the cyber-security data processing system 202 may be a data collection module 101 or a security monitoring device 100. The cyber-security data processing system 202 may receive user data for its consumers through channels such as customer database 204, internet connected device 212, account information system 226, and cyber-traffic event analysis system 222. The cyber-security data processing system 202 may
communicate with one or more network-based accounts to detect information associated with a consumer account being communicated through a network.

[25] In some embodiments, the cyber-security data processing system 202 may collect information from and transmit information to each of the various applications, databases, devices, and backend servers described in Figure 2. The cyber-security data processing system 202 may collect information about consumers such as their real-time activity and interactions, predict the likelihood of a data breach, and determine strategies utilizing the various channels of communication with the consumer so as to determine how to best engage the consumer and protect the consumer from future threats. For example, the cyber-security data processing system 202 may collect information about a local network associated with a consumer based on receiving a network scan from the security monitoring software 220. The cyber-security data processing system 202 may analyze historic account information received from the account information system 226 to determine the likelihood of a data breach based on risk factors known for consumers with similar habits and/or characteristics. The cyber-security data processing system 202 may determine that the user may be engaging in particularly risky behavior, and may determine when to contact the consumer and through which channel to contact the consumer to inform the consumer of the potential for a data breach. The cyber-security data processing system 202 may enable a plurality of different permutations of strategies such as the above example by being able to sense real-time consumer actions and consumer-related data flow through various different channels. By analyzing data relevant to that consumer, the cyber-security data processing system 202 may inform various channels that it is communicatively coupled to regarding consumer-associated risks.

[26] In some embodiments, the cyber-security data processing system 202 may communicate with a user (e.g., a consumer) and gather user data through banking application 218. The cyber-security data processing system 202 may collect user data from interactions of the user with the user interface of the banking mobile application 218. The banking application 218 may allow the user to manage account preferences,
manage financial accounts, view recent transactions, and/or review suspicious behavior. The cyber-security data processing system 202 may track interactions with banking applications and/or receive notifications from the applications. For example, a notification regarding a recent suspicious banking transaction may be sent from a banking server to the banking application 218 and (either from the banking server or via the banking application 218) forwarded to the cyber-security data processing system 202. This may cause the cyber-security data processing system 202 to inform the consumer of the suspicious activity.

[27] In some embodiments, a password manager 206 may assist the cyber-security data processing system 202 in determining the presence of consumer-associated accounts, and/or may assist the cyber-security data processing system 202 in determining the quality of credentials for the consumer-associated accounts. A risk-factor for a data breach may be a consumer who uses poor credentials (e.g., usernames, passwords, biometric information, etc.) for online accounts (e.g., weak passwords, using passwords for multiple accounts, a failure to use two-factor authentication, etc.). The password manager 206 may inform the cyber-security data processing system 202 of known accounts associated with the password manager 206, as well as the status of the credentials associated with those accounts. In some instances, the cyber-security data processing system 202 may compare the accounts known to the password manager 206 with other accounts known to the cyber-security data processing system 202 to determine what accounts are protected through password management.

[28] In some embodiments, the customer may interact with the cyber-security data processing system 202 using the user computing device 208, web application 224, and/or user mobile computing device 210. The user may be able to view their current security status, see updates regarding security issues, seek remediation of those issues, and/or undergo further training regarding security practices. In some instances, if a data breach occurs, the consumer may be presented with an option to file an insurance claim for the security breach via the cyber-security data processing system 202 and/or through an associated application.
In some embodiments, the cyber traffic event analysis system 222 may monitor user activity on social media networks, the Internet in general, or the dark web (e.g., network-enabled websites with restricted addresses or accessibility such that the sites are not accessible using standard means, such as websites with no domain names that are hidden from online search engines). In some instances, the cyber-traffic event analysis system 222 may determine how much of a consumer's confidential (e.g., private) information is available electronically. Confidential information may comprise identity information such as name or birthday, marital status, family members, education, employment histories, online identities (e.g., user names on a social media account), financial information (e.g., banking numbers, credit card numbers, etc.), traceable assets (real estate, vehicles, etc.), court records, or other such information. By searching for electronically available information, the system may determine a "digital footprint" (e.g., a trail of data and information, available electronically and associated with the consumer). For example, the cyber-traffic event analysis system 222 may determine that a consumer's home address is available on 3 social media sites, 5 public web pages, and 2 dark web pages. The cyber-traffic event analysis system 222 may also search for instances where confidential information has become available. For example, the cyber-traffic event analysis system may further determine that one of the dark web pages has a credit card ending in "XXXX" associated with the consumer's address. The cyber-traffic event analysis system 222 may inform the cyber-security data processing system 202 of its findings, and the cyber-security data processing system 202 may act on those findings. For example, the cyber-security data processing system 202 may determine that the credit card number corresponds to the consumer, and push an alert to an application on the user's mobile computing device 210 notifying the user that their credit card number may have been breached.

In some embodiments, in addition to collecting user information from mobile applications and web applications, user information for consumers may be collected from various other channels such as user computing device 208, user mobile computing device 210, and internet connected device 212. The cyber-security data
processing system 202 may determine devices associated with the consumer. The
cyber-security data processing system may determine characteristics of those devices,
such as their operating systems, update history, software on the devices, hardware
characteristics, and so forth. The cyber-security data processing system 202 may use
this information to determine if the number of devices and/or characteristics of the
devices indicate a heightened threat of a data breach.

[31] In some embodiments, the account information system 226 may maintain and
dynamically update records of accounts for a consumer. For example, the account
information system 226 may interface with social networking accounts associated
with the consumer. If an account is breached (or if suspicious activity is detected), the
cyber-security data processing system 202 may be notified. The cyber-security data
processing system 202 may then notify the consumer, such as by sending an alert to a
user computing device 208 and/or user mobile computing device 210.

[32] FIG. 3 illustrates a block diagram 300 of a central processing unit that collects
information from various information data sources to determine an online presence
for a consumer (e.g., the spread of information or "footprint" left by a consumer in
digital spaces). As shown in FIG. 3, the CSDPS 202 may communicate with a
plurality of information data sources 304a, 304b, … 304n to collect information
related to the consumer to determine next steps to best serve the consumer.

[33] In some embodiments, the cyber-security data processing system 202 may retrieve
information from the plurality of information data sources 304a-304n in order to
determine the digital presence of a consumer. The data retrieval engine 310 may be
configured to monitor (e.g., continuously monitor) each of the information data
sources 304a-304n and report data of interest from any one of these data sources to
the cyber-security data processing system 202. For example, the data retrieval engine
310 may monitor social media sources to determine if account information associated
with the consumer is detected. If the information is detected, it may be passed on to
the cyber-security data processing system 202 for analysis. In another example, the
data retrieval engine 310 may interface with one or more digital accounts (banking
accounts, social media accounts, digital storefronts, etc.) to determine if accounts are created, active, and/or in use. Account information may be passed on to the cyber-security data processing system 202.

[34] In some embodiments, the cyber-security data processing system 202 may calculate risk based on the data gathered from the information data sources 304a-304n. For example, the insurance rules processing engine 312 may analyze the data retrieved from information data sources 304a-304n by the data retrieval engine 310 according to preset rules and/or algorithms in order to determine the likelihood of a data breach based on the digital presence of the consumer.

[35] In some embodiments, the cyber-security data processing system 202 may determine when and through which means to notify an insurance consumer of the risks of a data breach and/or evidence of a data breach according to preset rules and strategies calculated from the data gathered from the information data sources 304a-n. For example, the user notification engine 314 may determine a time to contact the consumer with a message and/or notification generated by the cyber-security data processing system 202 upon analyzing the activities of the consumer and processing such activities according to risk matrices maintained by cyber-security data processing system 202.

[36] In some embodiments, the cyber-security data processing system 202 may manage the various activities of each consumer, and the status of various accounts associated with the consumer. For example, the information management system 316 may keep track of all of the information received from information data sources 304a-304n and may also manage a schedule of message delivery by communicating with the user notification engine 314. In another example, the cyber-security data processing system 202 may notify the user whenever an account is accessed at an unexpected time and/or from an unexpected location.

[37] In some embodiments, the cyber-security data processing system 202 may determine which channel to use to communicate the decision of a strategy computed at the
cyber-security data processing system 202. For example, the information delivery engine 318 may detect which mobile application accessible to the user is the most appropriate channel on which to deliver the type of information that is scheduled to be delivered to the insurance consumer and/or other target audience.

FIG. 4 illustrates a user interface 400 displaying an example rating screen for a digital safety score 405. In some examples, these user interfaces may be generated by an application server, web application 224, user computing device 208, and/or user mobile computing device 210. It should be understood that the user interface of FIG. 4 is designed to illustrate various features and aspects of the user interfaces and the system, and do not limit the visual appearance or layout of the user interfaces. The mobile computing device 210 may be a smartphone, and the user interface 400 may be part of a smartphone app. A shortcut may be presented on a home screen (or desktop screen) of an operating system executing the user interface 400.

A digital safety score 405 may be a rating and/or representation of different components which contribute to the risk of a data breach of an associated consumer. The digital safety score 405 may be a numeric value that indicates the risk of a data breach. While the description herein assumes a higher score reflects a lower chance of a data breach, any algorithm for determining the value may be used. For example, the digital safety score 405 may comprise a value from 0 to 200, where an algorithm determines the value such that a higher value indicates a lower risk of a data breach. In some instances, a lower number may indicate lower risk. For example, a value from 0 to 100 may be assigned, wherein the value approximates the chance of a significant data breach within the next year.

The components depicted in user interface 400 are merely exemplary components, and any number of components that affect the possibility of a data breach may be used. The components may be represented with shapes that correspond to their strength and/or impact. For example, triangles or wedges may be sized in proportion to their impact versus other components (e.g., larger shapes correspond to a larger impact than smaller shapes). In another example, shapes may vary in size based on the
risk associated with each item (e.g., a larger shape may indicate an area with higher associated risk). In some instances, a shaded ring or pie graph may be divided into different proportional sections for each component that contributes to the risk of a data breach. In some instances, a combination of the above may be used. For example, the width of wedges may indicate the proportion of the score, while the height may indicate whether the component has a positive or negative impact, and a ring around the wedges may indicate the proportion of a maximum score achieved.

A number of exemplary components are depicted in FIG. 4. An online presence component 415 may indicate the online presence of a consumer. For example, a consumer may have 48 different accounts detected across a range of Internet services. The CSDPS 202 may determine that the relatively high number of accounts increases the potential risk of a data breach. Accounts may be judged based on the type of account. For example, a large number of banking accounts may greatly increase the risk of a significant data breach, because a breach may result in important financial data being compromised. In another example, a large number of website accounts comprising only a username and password (such as accounts on a cookbook website, a news website, a sports website, etc.) may be weighted less than a smaller number of banking accounts, because the impact of a data breach to the consumer may be minimal compared to the impact of a breach regarding banking information. In some instances, the usage of usernames and/or passwords may be tracked and used to determine a component of the digital safety score 405. For example, a password manager may report that three passwords are used across 48 accounts. This may greatly increase the danger of a data breach, as a breach of a password across one account may affect a large number of other accounts. In some instances, this may increase the probability of a data breach, which may be reflected in the rating.

Some components may monitor devices and/or environments associated with a consumer. A network component 440 may indicate the quality of networking security associated with a consumer. The CSDPS 202 may receive information indicating the types of devices on a network (e.g., switches, routers, etc.), the configurations of the
devices (e.g., encryption methods used, wireless vs. wired connections, software updates installed, credentials required for access, etc.), and/or how many devices are connected. For example, the CSDPS 202 may communicate with a home network associated with the consumer to determine that the consumer has a wireless router with a non-default administrative password, a WPA2 encrypted SSID that is not broadcast, two connected wireless devices, and a connected wired device. The CSDPS 202 may determine a rating based on the strength of the network and/or the potential for the network to be breached. An antivirus component 420 may indicate the health of one or more devices associated with the consumer. An antivirus may decrease the probability of a data breach by protecting software and/or hardware from malicious intrusions. The digital safety score 405 may thus be increased for every device with an installed antivirus, and may be lowered if a problem is detected. A devices component 435 may indicate risks associated with the number of and/or quality of devices associated with a consumer. A consumer may be more at risk for a data breach if more devices with access to consumer accounts exist. For example, the CSDPS 202 may determine that an old, forgotten tablet with an outdated operating system is associated with the user. The tablet may present an intrusion point due to unpatched vulnerabilities. Thus, the tablet may reduce the digital safety score 405.

An applications component 430 may also impact the digital safety score 405. The CSDPS 202 may receive information from one or more connected services. For example, a credit monitoring service may report fraudulent activity on a credit card, which may decrease the digital safety score. In another example, a consumer identify protection service may provide information on whether any breaches have been detected by their service, which may affect the score.

A training component 425 may adjust the digital safety score 405 based on training conducted by the consumer. A consumer may be able to watch training videos, read articles, take quizzes, or listen to audio regarding cyber-security. For example, the user may be able to interact with the displayed training component to see options for training. If the user engages in training items, the user may be rewarded through an
increased digital safety score. This may help encourage the user to stay informed regarding best practices for cyber-security.

FIG. 5 depicts an exemplary training quiz 500 in accordance with one or more aspects described herein. In some instances, the user may first receive instructional content (such as watching a video with information related to cyber-security, do's and don'ts, and the like). The user may be presented with a quiz regarding safety features discussed in the video or other instructional content. The user may be rewarded if they answer the questions correctly (as this may indicate that the user understood the content and/or knows how to practice good cyber-security).

FIG. 6 depicts an exemplary breakdown screen for a component in accordance with one or more aspects described herein. In some instances, the user may be able to examine the various components of the digital safety score 405. Breakdowns of the various data items that contribute to each component may be available for the consumer to view, along with notifications and/or suggestions for improvement. For example, the online presence component 415 may be accessed to present an online presence breakdown screen 600, as depicted in FIG. 6. The online presence breakdown screen 600 may provide the consumer with a listing of accounts associated with the consumer or data on the Internet detected by the cyber-traffic event analysis system 222. In some instances, this listing may provide a listing of registered accounts according to the name of the account (e.g., name of cable company, bank, etc.). For example, the consumer may be able to view a list of known Internet accounts, and discover that the consumer has numerous online accounts which the consumer was unaware of. In another example, the consumer may discover that the home address of the consumer is readily available on a web-page. In some instances, the listing may identify accounts associated with credit card use, recurring payments, frequent use, the storage of personal and/or confidential information, and/or other such characteristics.

In some instances, accounts may be centrally consolidated and/or cancelled. Accounts may be consolidated in the listing, such as by providing a centralized login for
multiple accounts. For example, a service provider associated with the CSDPS 202 may provide a centralized login screen with a consolidated username and password. A consumer may select accounts from the listing of detected accounts with which to use the centralized login screen. The consumer may also select unwanted accounts from the listing for cancellation. In some instances, the CSDPS 202 may direct the consumer to a web page associated with each account for cancelling each account. In other instances, the CSDPS 202 may process the selections by coordinating with one or more services to cancel accounts. This may have the advantage of reducing the digital footprint for a consumer by reducing the number of active accounts.

FIG. 7 depicts a method for determining a value associated with a potential for data breach of a consumer's data. The value (e.g., a digital safety score) may present a consumer or marketplace consumer with a readily identifiable value corresponding to the risk of a data breach involving a consumer.

At step 705, the CSDPS 202 may initiate a scan for consumer accounts. The CSDPS 202 may request login information from the consumer. Accounts may be determined according to one or more methods. For example, the consumer may supply the CSDPS with identifying information, such as a name, date of birth, address, social security number, or other such information. The CSDPS may integrate with one or more services (such as social media websites, banking websites, etc.) which may inform the CSDPS 202 whether the identifying information corresponds to an account on each service. In another example, the consumer may register to receive a digital safety score. As part of the registration, the consumer may be presented with a list of accounts, and may be asked to give credentials for the accounts. In yet another example, the consumer may supply the CSDPS 202 with access to an aggregation service, such as a password manager, which may identify known accounts and/or credentials for each account. Some accounts, such as accounts with a credit monitoring service and/or identity protection service, may supply data indicating risk. In some instances, the CSDPS 202 may find account data across numerous services.
and bring the data from all the services together so that it may bind the data into a value in step 725.

[50] At step 710, the CSDPS 202 may scan for devices associated with the consumer. The CSDPS 202 may identify devices on a network associated with the consumer and/or devices associated with the consumer's credentials. For example, the CSDPS 202 may initiate a network scan which may identify devices along a network and information corresponding to each device (e.g., device type, model numbers, operating systems, software versions, applications installed on the devices, network capabilities, etc.).

[51] At step 715, the CSDPS 202 may search for digitally-available information associated with the consumer (e.g., an online presence associated with the consumer). The CSDPS 202 may initiate a scan for digitally-available information, such as by instructing the cyber-traffic event analysis system 222 to scan for consumer information (addresses, credit card numbers, credentials, social security numbers, etc.) that correspond to the consumer. In some instances, the cyber-traffic event analysis system may continually compile consumer data based on data found on the Internet. For example, the cyber-traffic event analysis system may monitor dark web pages for credit card numbers, addresses, phone numbers, etc. The CSDPS 202 may also collect activity data associated with the consumer. For example, the CSDPS 202 may track how often, on what devices, and/or where a consumer conducts banking transactions. A consumer may be penalized if the consumer conducts banking on a train, where other individuals may be able to more easily view the consumer's confidential banking information.

[52] At step 720, the CSDPS 202 may compare the consumer information with data known to correspond to the consumer. In some instances, the CSDPS 202 may determine if data compiled by the cyber-traffic event analysis system matches data associated with the consumer. For example, the CSDPS 202 may determine if a credit card number previously found on a dark web page and stored in a database of detected credit card numbers matches a credit card number entered by the consumer.
At step 725, the CSDPS 202 may determine a value associated with the consumer. The CSDPS 202 may use one or more algorithms to determine a value based on consumer accounts, consumer devices, online presence data, or other collected information. The CSDPS 202 may compare the compiled data against risk matrices to determine the likelihood of a data breach based on the collected data. For example, a user with a large number of devices and accounts may have a high probability of a data breach and be assigned a low value.

At step 730, the CSDPS 202 may update a marketplace with the value. Risk information (e.g., a value and/or the information from which the value is derived) may be a valuable tool for determining the risk of a data breach associated with a consumer. For example, the value may indicate that there is a 20% chance that a consumer will fall victim to credit card fraud within the next six months.

A marketplace may be established for buying and selling risk information. For instance, an insurance marketplace may allow insurance providers to access risk information from the CSDPS 202. Insurance providers and/or underwriters may establish cyber-fraud insurance policies based on the risk information. For example, an insurance provider may offer an insurance policy to the consumer that protects against fraudulent transactions based on the risk information. If a consumer incurs financial damage as a result of a data breach (for example, the consumer is subjected to credit card fraud), the insurance policy may compensate the consumer for some or all financial losses incurred.

Premiums and/or deductibles for insurance policies may be established based on the risk information and/or value associated with a potential for data breach of a consumer's data. For example, a consumer with a high value may be charged a higher premium than a consumer with a low value.

In some instances, the risk information may be collected and used to determine behavioral patterns for a class of consumer. Over time, the CSDPS 202 may determine the behavioral patterns based on detecting associations between different
data points known to the CSDPS 202. For example, the CSDPS 202 may determine that individuals with more than two credit card numbers detected on the Internet have a 65% chance of credit card fraud, while individuals with two or less credit card numbers detected on the Internet have a 38% chance of credit card fraud. The CSDPS 202 may continually iterate on this information to determine more and/or more accurate associations and/or patterns. For example, using data collected over time, the CSDPS 202 may determine that individuals with at least 5 active social networking accounts have a 15% greater chance of suffering from tax fraud than individuals with less than 5 active social networking accounts. Thus, the CSDPS 202 may determine an increased chance of tax fraud when a consumer registers a fifth social networking account (and, in some instances, provide a notification to a user and/or service provider after the fifth social networking account is registered).

In some instances, the determined, resultant behavioral data representing the behavioral patterns and/or the data used to determine behavioral patterns may be made available through the marketplace. A database of patterns may be made available detailing the risks associated with given behaviors (e.g., the risk of a data breach based on a given digital footprint). An insurer may pay to have access to a marketplace of the data in order to better tailor insurance products for a consumer based on associated risk. For example, the insurer may increase premiums for all customers by 7% because the data used to determine behavioral patterns indicates an overall 7% increase in cyber-crime in the past 18 months. In some instances, a governmental entity, such as law enforcement, may subscribe to the marketplace in order to determine how best to predict, identify, and/or react to cyber-crime. Data may also be used for advertising purposes. An advertiser may use the data to associate online activity with demographic information for targeted advertising. For example, an advertiser may determine a demographic of consumers aged 20-28 with at least 6 social networking accounts in order to conduct a targeted advertising campaign for a new social network. In another example, a post-card company may determine a list of consumers with no social networking accounts for mailing an advertisement comprising a selection of post-cards.
[59] In some instances, access to the marketplace may be restricted and/or incur a fee. For example, a fee may be charged to access risk information collected by the CSDPS 202. In some instances, the CSDPS 202 may collect information from a variety of sources (e.g., credit monitoring services, identity theft protection services, consumer information protection services, etc.), and store the combined information in a database. In some instances, a separate fee may be charged for access to only a subset of the database information.

[60] At step 735, the CSDPS 202 may determine if an action event has been detected. An action event may comprise a detected change in a consumer account and/or detection of a data breach. For example, the cyber-traffic event monitoring system 222 may detect that a credit card number associated with a consumer with a known value has been published on a website.

[61] In some instances, an action event may be an action taken by the consumer. A consumer may register a new account online, open up a new financial service account, start using a password manager, connect a new device, or undergo cyber-security training. As a result of the action, the CSDPS 202 may wish to adjust the value. For example, by adding additional accounts online, the consumer may be more susceptible to a data breach and the value may be lowered. In another example, the consumer may perform cyber-security training, and may be rewarded with a higher value.

[62] At step 740, The CSDPS 202 may notify the consumer of the action event. To reduce the impact of a data breach, it may be advantageous to notify the consumer and/or services associated with the data breach. For example, the CSDPS 202 may trigger a notification to appear on a user mobile computing device 210 indicating that credentials have been leaked for an account. In another example, the CSDPS 202 may notify a credit card company that a credit card number for the consumer was detected on the dark web. The consumer and/or service provider may then take action to reduce any potential damage resulting from the data breach.
At step 745, the CSDPS 202 may adjust the value. Information indicating if a breach is more or less likely to occur may affect a value. In some instances, an actual data breach may indicate that a breach is more likely to occur in the future, lowering the value. For example, if a data breach has occurred, the value may be lowered. In another example, a value may be raised when a user deletes old social media accounts that the consumer no longer uses. In yet another example, a value may be raised when a user enacts stronger privacy policies on accounts, such as social media accounts. After adjusting the value, the CSDPS 202 may return to step 730 to update the marketplace with the new risk information.

Aspects of the invention have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional in accordance with aspects of the invention.
What is claimed is:

1. A cyber-security system comprising a cyber-traffic event analysis system and a cyber-security data processing system:
   wherein the cyber-traffic event analysis system is configured to:
   monitor a communications network for confidential information associated with a consumer account associated with a consumer;
   detect evidence of a data breach of the confidential information associated with the consumer account as a result of the monitoring; and
   report the evidence of the data breach to the cyber-security data processing system;
   wherein the cyber-security data processing system is configured to:
   receive the evidence of the data breach associated with the consumer account;
   determine a probability of a future impact to the consumer based on the evidence of the data breach; and
   adjust a value based on the probability.

2. The cyber-security system of claim 1, wherein the evidence of the data breach comprises a credit card number.

3. The cyber-security system of claim 1, wherein the evidence of the data breach comprises credentials associated with the consumer account.

4. The cyber-security system of claim 1, wherein the communications network comprises the Internet.

5. The cyber-security system of claim 1, wherein the cyber-security data processing system is further configured to determine the value based on an online presence of the consumer.
6. The cyber-security system of claim 1, wherein the cyber-security data processing system is further configured to:
   - publish the value on an online marketplace;
   - receive a request for the value; and
   - transmit the value to a service provider in response to the request.

7. The cyber-security system of claim 1, wherein the cyber-security data processing system is further configured to:
   - receive an indication that the consumer has undergone cyber-security training;
   - adjust the value based on the cyber-security training; and
   - transmit the adjusted value for presentation to the consumer.

8. A method comprising:
   - determining, by a security monitoring device, one or more accounts comprising confidential information associated with a consumer;
   - scanning, by the security monitoring device, a local network associated with the consumer for one or more local devices on the local network;
   - monitoring, by the security monitoring device, an external network for a data breach associated with the confidential information;
   - determining, by the security monitoring device, a value based on the determining the one or more accounts, the scanning the local network, and the monitoring the external network; and
   - transmitting, by the security monitoring device, the value for presentation to the consumer.

9. The method of claim 8, wherein the monitoring the external network for the data breach comprises monitoring one or more Internet sites for the confidential information.

10. The method of claim 8, further comprising:
    - publishing the value on an online marketplace;
receiving a request for the value; and
transmitting the value to a service provider in response to the request.

11. The method of claim 8, further comprising:
   detecting, after the transmitting the value, a new data breach associated with the
   confidential information;
   adjusting the value based on the detecting; and
   transmitting the adjusted value for presentation to the consumer.

12. The method of claim 8, wherein the determining the value further comprises
determining the value further based on information received from a credit monitoring service.

13. The method of claim 8, further comprising:
   receiving an indication that the consumer has undergone cyber-security training;
   adjusting the value based on the cyber-security training; and
   transmitting the adjusted value for presentation to the consumer.

14. A cyber-security data processing system comprising a cyber-traffic event analysis
system and a cyber-security data processing system:
   a processor;
   a memory unit storing computer-executable instructions, which when executed by the
   processor, cause the cyber-security data processing system to:
   - monitor a communications network for confidential information
     associated with a consumer;
   - detect one or more instances of the confidential information on the
     communications network as a result of the monitoring; and
   - receive additional information associated with the consumer from a service
     provider;
determine a probability of a future data breach based on the one or more instances and the additional information; and
adjust a value based on the probability.

15. The cyber-security data processing system of claim 14, wherein the cyber-security data processing system further stores computing-executable instructions, which when executed by the processor, cause the cyber-security data processing system to:
   publish the value on an online marketplace;
   receive a request for the value; and
   transmit the value to an insurance provider in response to the request.

16. The cyber-security data processing system of claim 14, wherein the service provider comprises a credit monitoring service.

17. The cyber-security data processing system of claim 14, wherein the cyber-security data processing system further stores computing-executable instructions, which when executed by the processor, cause the cyber-security data processing system to transmit the value to a device associated with the consumer.

18. The cyber-security data processing system of claim 17, wherein the cyber-security data processing system further stores computing-executable instructions, which when executed by the processor, cause the cyber-security data processing system to:
   detect, after the transmitting the value, a new instance of the confidential information;
   adjust the value based on detecting the new instance; and
   transmit the adjusted value for presentation to the consumer.

19. The cyber-security data processing system of claim 18, wherein the adjusted value is presented to the consumer as a number displayed via a cyber-security application on a mobile computing device.
20. The cyber-security data processing system of claim 14, wherein the cyber-security data processing system further stores computing-executable instructions, which when executed by the processor, cause the cyber-security data processing system to:
   receive an indication that the consumer has undergone cyber-security training;
   adjust the value based on the cyber-security training; and
   transmit the adjusted value for presentation to the consumer.
FIG. 3

Cyber-Security Data Processing System

- Information Management System 316
- Information Delivery Engine 318
- Data Retrieval Engine 310
- Rules Processing Engine 312
- User Notification Engine 314

Information Data Source 304a
Information Data Source 304b
Information Data Source 304n
Cyber-Safety
Training Quiz

What is safer?

- A long password unique to you
- A very short password with random letters

FIG. 5
Online Presence Breakdown

Click to View:

- 48 Social Media Accounts
- 13 Banking Accounts
- 28 Web Domains Mentioning Name and Address

FIG. 6
Start

705
Scan For Consumer Accounts

710
Scan for Consumer Devices

715
Search for Consumer Information

720
Compare Consumer Information with Known Data

725
Determine Value

730
Update Marketplace

735
Detect Action Event

740
Provide Notification

745
Adjust Value

FIG. 7
This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. 
   - Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:

2. 
   - Claims Nos.: because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. 
   - Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

This International Searching Authority found multiple inventions in this international application, as follows:

- "Please See in Extra Sheet" -

1. 
   - As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. 
   - As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. 
   - As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. 
   - No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-7

Remark on Protest

- The additional search fees were accompanied by the applicant’s protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant’s protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06F 21/55, 21/60; H04W 12/12 (2017.01)
CPC - H04L 63/1408, 63/1416, 63/1425, 63/20; G06Q 30/0185; H04W 12/12; G06F 21/50, 21/554, 21/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>US 2016/0065614 A1 (THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK) 03 March 2016; figure 1; paragraphs [0023], [0032], [0035], [0039].</td>
<td>1-5, 7</td>
</tr>
<tr>
<td>Y</td>
<td>US 201 1/0166968 A1 (COULTER, D) 07 July 201 1; paragraphs [0266], [0267].</td>
<td>1-5, 7</td>
</tr>
<tr>
<td>Y</td>
<td>US 2014/0262977 A1 (SOCURE INC.) 18 September 2014; paragraphs [0019], [0023], [0041].</td>
<td>5</td>
</tr>
<tr>
<td>Y</td>
<td>US 2013/0179360 A1 (EZSHIELD, INC.) 11 July 2013; paragraphs [05624][0529], [0553], [0555].</td>
<td>7</td>
</tr>
<tr>
<td>A</td>
<td>US 201 3/02981 92 A1 (KUMAR, S et al) 07 November 201 3; entire document.</td>
<td>1-7</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "E" earlier application or patent but published on or after the international filing date
  "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  "O" document referring to an oral disclosure, use, exhibition or other means
  "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"A" document member of the same patent family

Date of the actual completion of the international search: 18 July 2017 (16.07.2017)

Date of mailing of the international search report: 5 SEP 2017

Name and mailing address of the ISA/
Mail Stop PCT, Attn: IASUS, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-8300

Authorized officer: Shane Thomas
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)
INTERNATIONAL SEARCH REPORT

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-7 are directed towards a cyber security system detecting a data breach and determining a future impact to a consumer based on the data breach.

Group II: Claims 8-13 are directed towards a method of determining a value based on scanning and monitoring an internal and external network for consumer accounts, and presenting the value to the consumer.

Group III: Claims 14-20 are directed towards receiving consumer information from a service provider and determining a probability of a future data breach based on the information.

The inventions listed as Groups I-III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least: report the evidence of the data breach to the cyber-security data processing system; wherein the cyber-security data processing system is configured to: receive the evidence of the data breach associated with the consumer account; determine a probability of a future impact to the consumer based on the evidence of the data breach; and adjust a value based on the probability, which are not present in Groups II-III.

The special technical features of Group II include at least: determining, by a security monitoring device, one or more accounts comprising confidential information associated with a consumer; determining, by the security monitoring device, a value based on the determining the one or more accounts, the scanning the local network, and the monitoring the external network; and transmitting, by the security monitoring device, the value for presentation to the consumer, which are not present in Groups I and III.

The special technical features of Group III include at least: a processor; a memory unit storing computer-executable instructions, which when executed by the processor, cause the cyber-security data processing system to: and receive additional information associated with the consumer from a service provider; determine a probability of a future data breach based on the one or more instances and the additional information; and adjust a value based on the probability, which are not present in Groups II-III.

The common technical features shared by Groups I-III are: a cyber-security system comprising a cyber-traffic event analysis system and a cybersecurity data processing system; wherein the cyber-traffic event analysis system is configured to: monitor a communications network for confidential information associated with a consumer account associated with a consumer; scanning, by the security monitoring device, a local network associated with the consumer for one or more local devices on the local network; and transmitting, by the security monitoring device, the value for presentation to the consumer as a result of the monitoring; detect one or more instances of the confidential information on the communications network as a result of the monitoring.

However, these common features are previously disclosed by US 2016/0065614 to THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK (hereinafter "Columbia"). Columbia discloses a cyber-security system comprising a cyber-traffic event analysis system and a cybersecurity data processing system; wherein the cyber-traffic event analysis system is configured to: monitor a communications network for confidential information associated with a consumer account associated with a consumer (monitoring a communications network for user actions in a computing environment indicative of attacks stealing a bank customer’s account information (confidential); figure 1; paragraphs [0023], [0032], [0035], [0039]); scanning, by the security monitoring device, a local network associated with the consumer for one or more local devices on the local network (continuously monitoring when decoy information has been accessed (scanning), by the security and monitoring computer, a communications network for an external attacker that obtains internal network access (local network) for actions in a computing environment indicative of attacks stealing a bank customer’s account information (confidential); figure 1: paragraphs [0023], [0032], [0035], [0039], [0040]); detecting evidence of a data breach of the confidential information associated with the consumer account as a result of the monitoring (detect significant behavior differences which can be indicative (evidence) of a security breach or malicious intent to steal a bank customer’s account information by continuously monitoring user behavior (result of the monitoring); paragraphs [0017], [0032]) detect one or more instances of the confidential information on the communications network as a result of the monitoring (monitoring a communications network for user actions in a computing environment indicative of attacks stealing a bank customer’s account information (detecting instances of confidential information); figure v. paragraphs [0023], [0032], [0035], [0039]).

Since the common technical features are previously disclosed by the Columbia reference, these common features are not special and so Groups I-III lack unity.