

A (sample) computerized system for publishing the daily currency exchange rates

The Treasury Department has constructed a computerized system that publishes the daily exchange rates of the local currency on the Web. The rates are published on a daily basis and present the exchange relation of the local currency with the ten leading world currencies (e.g. USD, Euro, GBP, Rubles, etc.). The updated daily rates data are used by the public for carrying out monetary transactions, changing money and accepting investment decisions.

The exchange rates table is published on a Web site that is open to the public. The access is free of charge. The daily update of the rates is performed by economists of the Treasury Department. The history of the rates is kept in the currency rates database for 5 years. Each daily rate entry includes the date, the exchange rates and the name of the specific economist that submitted the data. Users may request the rates for any specific day during last five year period.

The economist activities e.g. connecting to database and updating the rates are logged in the database.

Architecture:

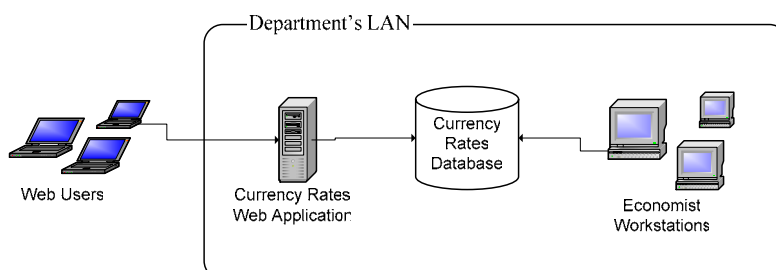
The Web site that publishes the rate pages to the public is based on Microsoft IIS 6 platform, which runs on Microsoft Server 2003 computer.

The database that stores the rates data is Microsoft SQL Server 2000 running on a stand alone Microsoft Server 2003 computer.

The rates update application that is used by the economists is a Windows desktop application installed on Windows XP workstations.

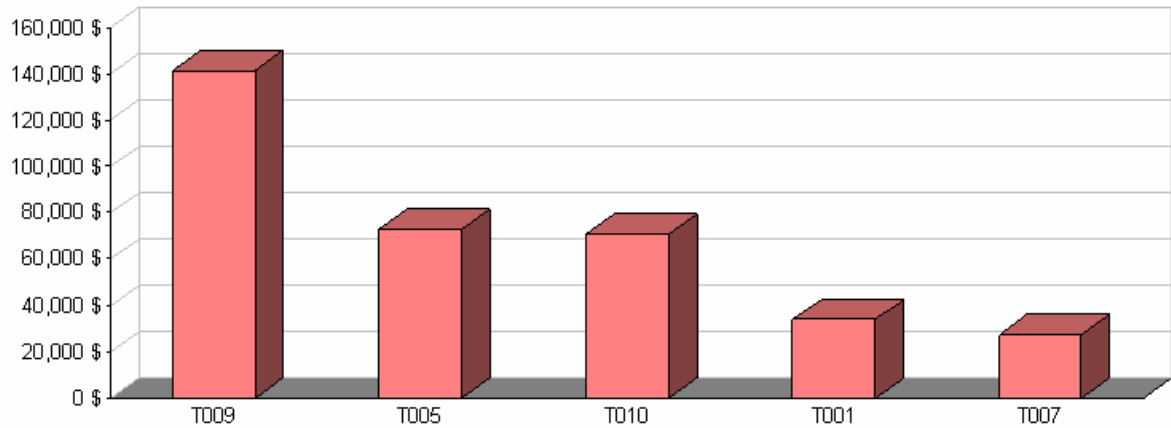
The Web server and the economist workstation are connected to the database server through the department local area network.

The following figure presents the schematic view of the system:



Top Threats by Current Risk

ID	Name	Value at Risk
T009	A malicious economist forges currency rates	141,226 \$
T005	Denial of Service attack on the web site	72,957 \$
T010	Hostile countries may manipulate currency rates by recruiting economists	70,613 \$
T001	Hacker corrupts database by injecting malicious SQL statements in input fields	34,135 \$
T007	Hacker uses HTTP requests to get access to OS resources of the Web server	27,451 \$



Detailed Vulnerabilities

V001 The Web server and database server machines may be accessed through the internet

Description:

Anyone can reach the server machines by scanning the organization network from the internet. This vulnerability can be mitigated by controlling incoming network traffic.

Relevant Threats:

- T005 Denial of Service attack on the web site
- T006 Malicious hacker corrupts database by connecting to database server directly from internet

Relevant Countermeasures:

- C001 Install firewall

V002 The Web server and database server machines may be accessed through the LAN

Description:

Unauthorized personnel that have access to LAN can reach server machines.

Relevant Threats:

- T004 Malicious insider connects to database via LAN for corrupting and/or altering the data

Relevant Countermeasures:

- C002 Physically protect access to local network wiring
- C003 Enforce quality passwords policy for protecting each of the machines on the network

V004 The database passwords may be sniffed from the LAN when establishing connection to database server

Description:

Insider may learn passwords that are transferred in plain text by using sniffing equipment.

Relevant Threats:

- T004 Malicious insider connects to database via LAN for corrupting and/or altering the data

Relevant Countermeasures:

- C002 Physically protect access to local network wiring
- C004 Use windows integrated authentication for database logins

V006 SQL server is prone to injection of malicious code via Web pages

Description:

Malicious SQL code may be injected via input fields and may cause damage to the data and the structure of the database.

Relevant Threats:

- T001 Hacker corrupts database by injecting malicious SQL statements in input fields of the rates Web page

Relevant Countermeasures:

- C005 Database login accounts should be given the minimal rights that are necessary for their functionality

- C006 Implement validation of input fields in rates web pages
- C007 Enforce data access via stored procedures with formal parameters content validation
- C009 Enforce security code review

V007 MS Server 2003 and IIS 6.0 have shortcomings that enable exploitation of OS resources via HTTP protocol

Description:

Search for updated security exploits such as buffer overrun, url canonicalization and other weaknesses that enable malicious activities through HTTP requests.

Relevant Threats:

- T007 Hacker uses HTTP requests to get access to OS resources of the Web server

Relevant Countermeasures:

- C008 Enforce policy of downloading and deployment of latest security patches for OS, database and Web server

V009 Unauthorized user of the economist application can enter the rates

Relevant Threats:

- T002 Insider corrupts database by injecting malicious SQL statements in input fields of the economist's application

Relevant Countermeasures:

- C004 Use windows integrated authentication for database logins
- C005 Database login accounts should be given the minimal rights that are necessary for their functionality
- C010 Economist application login should be bound with Windows login
- C012 Enforce economist password protection policy

V011 Web servers are exposed to DoS attacks

Description:

A well-known vulnerability.

Relevant Threats:

- T005 Denial of Service attack on the web site

Relevant Countermeasures:

- C013 Install anti-DoS appliance

V012 Economist can set currency rates and modify historical currency rates data

Description:

Economist has a mandate to alter and correct rates data.

Relevant Threats:

- T009 A malicious economist forges currency rates
- T010 Hostile countries may manipulate currency rates by recruiting economists

Relevant Countermeasures:

- C016 Develop module for logging of economists' activities
- C017 Develop two-phase protocol for changing historical rates data that involves managerial personnel
- C018 Develop fraud detection mechanism

C020 Set severe punishments in law against insiders economical crimes

V013 Economist personal weaknesses may be exploited by hostile parties

Relevant Threats:

T010 Hostile countries may manipulate currency rates by recruiting economists

Relevant Countermeasures:

C019 Security officer will have mandate to assure the personal integrity of economists

Detailed Assets by Value

A006 The stability of the state's economy

Description:

The state's economy depends on the reputation of the Treasury Department and the currency rate system is a major factor in gaining (or losing) this reputation.

Weighted Value: 1,000,000 \$ 68.3 % of total assets

Risk: Maximal: 12.0 % Current: 12.0 % Minimal: 5.0 %

Relevant Threats:

- T009 A malicious economist forges currency rates
Level of Damage: 16. % Probability: 0.50
- T010 Hostile countries may manipulate currency rates by recruiting economists
Level of Damage: 16. % Probability: 0.25

A005 The trust of the public in the exchange rates service

Description:

If rates are inaccurate or corrupted and the service is not provided in a stable manner, the public will not trust the service and may look for alternative options causing looser affect of the Treasury Department on the state's economy.

Weighted Value: 250,000 \$ 17.1 % of total assets

Risk: Maximal: 93.4 % Current: 57.7 % Minimal: 25.5 %

Relevant Threats:

- T005 Denial of Service attack on the web site
Level of Damage: 16. % Probability: 0.82
- T007 Hacker uses HTTP requests to get access to OS resources of the Web server
Level of Damage: 66. % Probability: 0.66
- T009 A malicious economist forges currency rates
Level of Damage: 49. % Probability: 0.50
- T010 Hostile countries may manipulate currency rates by recruiting economists
Level of Damage: 49. % Probability: 0.25

A003 The accuracy and integrity of the exchange rates data

Description:

The exchange rates must be accurate. If rates are inaccurate or corrupted, a financial damage may be caused to the business entities that base their transactions on the data. The value of the asset is the maximal annual damage that can be caused by manipulating the rates data.

Weighted Value: 100,000 \$ 6.8 % of total assets

Risk: Maximal: 132.3 % Current: 58.5 % Minimal: 0.0 %

Relevant Threats:

- T001 Hacker corrupts database by injecting malicious SQL statements in input fields of the rates Web page
Level of Damage: 90. % Probability: 0.33
- T002 Insider corrupts database by injecting malicious SQL statements in input fields of the economist application

- Level of Damage: 90. % Probability: 0.16
- T004 Malicious insider connects to database via LAN for corrupting and/or altering the data
Level of Damage: 90. % Probability: 0.16
- T006 Malicious hacker corrupts database by connecting to database server directly from internet
Level of Damage: 90. % Probability: 0.82

A002 The availability of the daily exchange rates service

Description:

If the website goes down, the economical transactions that depend on the exchange rates cannot be realized since users will not be able to request the rates data. The asset's value is the maximal liability for this damage as set by the Treasury's regulations.

Weighted Value: 100,000 \$ 6.8 % of total assets

Risk: Maximal: **83.7 %** Current: **48.0 %** Minimal: **15.1 %**

Relevant Threats:

- T005 Denial of Service attack on the web site
Level of Damage: 49. % Probability: 0.82
- T007 Hacker uses HTTP requests to get access to OS resources of the Web server
Level of Damage: 66. % Probability: 0.66

A001 The confidentiality of economists' personal information

Description:

Exposure of economists personal data may enable blackmailing the economists and manipulating the exchange rates by malicious parties.

Weighted Value: 15,000 \$ 1.0 % of total assets

Risk: Maximal: **127.7 %** Current: **45.7 %** Minimal: **0.0 %**

Relevant Threats:

- T001 Hacker corrupts database by injecting malicious SQL statements in input fields of the rates Web page
Level of Damage: 90. % Probability: 0.33
- T004 Malicious insider connects to database via LAN for corrupting and/or altering the data
Level of Damage: 100 % Probability: 0.16
- T006 Malicious hacker corrupts database by connecting to database server directly from internet
Level of Damage: 100 % Probability: 0.82

Detailed Threats by Current Risk

T009 A malicious economist forges currency rates

Description:

Malicious economist may join forces with other parties for faking currency rates. Since many economical transactions are based on currency rates, this forgery can lead to enormous fraud transactions that may damage the stability of the state's economy and the trust of the public.

Damage: 19.3 % from total system assets

Probability: 0.50

Risk: Maximal: 9.6 % Current: 9.6 % Minimal: 4.8 %

Maximal Mitigation Available: 50.0 %

Threatened Assets:

- A005 The trust of the public in the exchange rates service
Level of Damage: 49 %
- A006 The stability of the state's economy
Level of Damage: 16 %

Exploited Vulnerabilities:

- V012 Economist can set currency rates and modify historical currency rates data
Economist has a mandate to alter and correct rates data.

Recommended Countermeasures:

- C016 Develop module for logging of economists' activities
The module will log all activities of logged-in users that use the economist application.
Included in Mitigation Set: V
- C017 Develop two-phase protocol for changing historical rates data that involves managerial
Included in Mitigation Set: V
- C018 Develop fraud detection mechanism
The fraud detection module will scan database and economist activity log.
Included in Mitigation Set: V
- C020 Set severe punishments in law against insiders' economical crimes
Included in Mitigation Set: V

Entry Points:

- E002 The economist desktop application for updating rates

Attacker Types:

- K004 Economist

Tags:

- G008 Business procedures

T005 Denial of Service attack on the web site

Description:

DoS attack prevents rates from being available to public.

Damage: 6.1 % from total system assets

Probability: 0.82

Risk: Maximal: 5.0 % Current: 5.0 % Minimal: 0.9 %

Maximal Mitigation Available: 82.0 %

Threatened Assets:

- A002 The availability of the daily exchange rates service
Level of Damage: 49 %
- A005 The trust of the public in the exchange rates service
Level of Damage: 16 %

Exploited Vulnerabilities:

- V001 The Web server and database server machines may be accessed through the internet. Anyone can reach the server machines by scanning the organization network from the internet. This vulnerability can be mitigated by controlling incoming network traffic.
- V011 Web servers are exposed to DoS attacks - a well-known vulnerability.

Recommended Countermeasures:

- C001 Install firewall
The network is secured by using industry standard firewall, which is configured to block traffic from the internet to the local area network, excluding HTTP requests to Exchange Rates Web site. The cost of the implementation is the one time cost of the firewall purchase and deployment.
Included in Mitigation Set: V
- C013 Install anti-DoS appliance
The cost estimation is based on the one time expense for purchasing and deploying the appliance by system administration.
Included in Mitigation Set: V

Entry Points:

- E001 The rates page of the Web application

Attacker Types:

- K003 Hacker

Tags:

- G005 Networking
- G006 Application servers

T010 Hostile countries may manipulate currency rates by recruiting economists

Description:

Economical sabotage is part of war arsenal between states.

Damage: 19.3 % from total system assets

Probability: 0.25

Risk: Maximal: 4.8 % Current: 4.8 % Minimal: 1.2 %

Maximal Mitigation Available: 75.0 %

Threatened Assets:

- A005 The trust of the public in the exchange rates service
Level of Damage: 49 %
- A006 The stability of the state's economy
Level of Damage: 16 %

Exploited Vulnerabilities:

- V012 Economist can set currency rates and modify historical currency rates data

Economist has a mandate to alter and correct rates data.
V013 Economist personal weaknesses may be exploited by hostile parties

Recommended Countermeasures:

- C016 Develop module for logging of economists' activities
The module will log all activities of logged-in users that use the economist application.
Included in Mitigation Set: V
- C017 Develop two-phase protocol for changing historical rates data that involves managerial
Included in Mitigation Set: V
- C018 Develop fraud detection mechanism
The fraud detection module will scan database and economist activity log.
Included in Mitigation Set: V
- C019 Security officer will have mandate to assure the personal integrity of economists
Included in Mitigation Set: V
- C020 Set severe punishments in law against insiders' economical crimes
Included in Mitigation Set: V

Entry Points:

E002 The economist desktop application for updating rates

Attacker Types:

K005 State's enemies

Tags:

G008 Business procedures

T001 Hacker corrupts database by injecting malicious SQL statements in input fields of the rates Web page

Description:

A sophisticated web attacker may reverse engineer the client side code of the web page and insert malicious sql to be submitted as the value of the date field hoping that it will be transferred to the database 'as is'. The code may include instructions for deleting database objects, altering the data itself or querying the information.

Damage: 7.1 % from total system assets

Probability: 0.33

Risk: Maximal: 2.3 % Current: 2.3 % Minimal: 0.0 %

Maximal Mitigation Available: 100.0 %

Threatened Assets:

- A001 The confidentiality of economists' personal information
Level of Damage: 90 %
- A003 The accuracy and integrity of the exchange rates data
Level of Damage: 90 %

Exploited Vulnerabilities:

V006 SQL server is prone to injection of malicious code via Web pages
Malicious SQL code may be injected via input fields and may cause damage to the data and the structure of the database.

Recommended Countermeasures:

C005 Database login accounts should be given the minimal rights that are necessary for their Web application account used for retrieving daily rates is assigned with read only

permissions. Economist account is given update privileges only on rates data. DB administrator is the only account with full rights on the database that can access and modify data. The cost reflects administration effort.

Included in Mitigation Set: V

C006 Implement validation of input fields in rates web pages

For example: validate the input to the date field in the rates page. The cost expresses the one time effort for developing this software feature.

Included in Mitigation Set: V

C007 Enforce data access via stored procedures with formal parameters content validation

Data in database should be manipulated only via stored procedures. The parameters of the stored procedures should be validate for their content before executing the stored procedure. The cost here is the one time effort for developing this software feature.

Included in Mitigation Set: V

C009 Enforce security code review

Review all system's source codes according to 'secure code writing' industry standards. The cost here is the one time effort for implementing this software review.

Included in Mitigation Set: V

Entry Points:

E001 The rates page of the Web application

Attacker Types:

K003 Hacker

Tags:

G004 Data

G006 Application servers

T007 Hacker uses HTTP requests to get access to OS resources of the Web server

Description:

The attack is performed using exploits that are regularly discovered in web server. The hacker may change the application home page, curse the government etc...

Damage: 15.8 % from total system assets

Probability: 0.66

Risk: Maximal: 10.4 % Current: 1.9 % Minimal: 1.9 %

Maximal Mitigation Available: 82.0 %

Threatened Assets:

A002 The availability of the daily exchange rates service

Level of Damage: 66 %

A005 The trust of the public in the exchange rates service

Level of Damage: 66 %

Exploited Vulnerabilities:

V007 MS Server 2003 and IIS 6.0 have shortcomings that enable exploitation of OS resources via HTTP protocol and search for updated security exploits such as buffer overrun, url canonicalization and other weaknesses that enable malicious activities through HTTP requests.

Recommended Countermeasures:

C008 Enforce policy of downloading and deployment of latest security patches for OS, database
The current security patches for all software infrastructures in the system should be maintained. The cost estimation is based on the yearly effort for deploying the patches by system administration.

Included in Mitigation Set: V

Entry Points:

E001 The rates page of the Web application

Attacker Types:

K003 Hacker

Tags:

G013 Operating System

G006 Application servers

T004 Malicious insider connects to database via LAN for corrupting and/or altering the data

Description:

The connection is established from a machine on local area network

Damage: 7.2 % from total system assets

Probability: 0.16

Risk: Maximal: 1.2 % Current: 1.2 % Minimal: 0.0 %

Maximal Mitigation Available: 100.0 %

Threatened Assets:

A001 The confidentiality of economists' personal information

Level of Damage: 100 %

A003 The accuracy and integrity of the exchange rates data

Level of Damage: 90 %

Exploited Vulnerabilities:

V002 The Web server and database server machines may be accessed through the LAN

Unauthorized personnel that have access to LAN can reach server machines.

V004 The database passwords may be sniffed from the LAN when establishing connection to database server

Insider may learn passwords that are transferred in plain text by using sniffing equipment.

Recommended Countermeasures:

C002 Physically protect access to local network wiring

If network is compromised, sensitive data could be viewed as a result of direct attacks on database server. The cost of the physically protection of the LAN is a one time expense.

Included in Mitigation Set: V

C003 Enforce quality passwords policy for protecting each of the machines on the network

Network users should choose strong passwords that are hard to guess or discover by brute force means. The cost expresses the yearly effort of enforcing the password policy by system administration.

Included in Mitigation Set: V

C004 Use windows integrated authentication for database logins

This type of secured logging protocol requires the installation of Windows domain controller + Active Directory + backup domain controller. The cost expresses the one time expense for purchasing the software and the continuous deployment effort by system administration.

Included in Mitigation Set: V

Entry Points:

E003 A computer machine on the LAN

Attacker Types:

K002 Insider

Tags:

- G004 Data
- G005 Networking

T002 Insider corrupts database by injecting malicious SQL statements in input fields of the economist application

Description:

The insider may be a malicious economist or an unauthorized person who took control on an economist station

Damage: 6.1 % from total system assets

Probability: 0.16

Risk: Maximal: 1.0 % Current: 1.0 % Minimal: 0.0 %

Maximal Mitigation Available: 100.0 %

Threatened Assets:

- A003 The accuracy and integrity of the exchange rates data
Level of Damage: 90 %

Exploited Vulnerabilities:

- V009 Unauthorized user of the economist application can enter the rates database

Recommended Countermeasures:

- C004 Use windows integrated authentication for database logins
This type of secured logging protocol requires the installation of Windows domain controller + Active Directory + backup domain controller. The cost expresses the one time expense for purchasing the software and the continuous deployment effort by system administration.
[Included in Mitigation Set:](#) V
- C005 Database login accounts should be given the minimal rights that are necessary for their
Web application account used for retrieving daily rates is assigned with read only permissions. Economist account is given update privileges only on rates data. DB administrator is the only account with full rights on the database that can access and modify data. The cost reflects administration effort.
[Included in Mitigation Set:](#) V
- C010 Economist application login should be bound with Windows login
The cost here is the one time effort for developing this software feature.
[Included in Mitigation Set:](#) V
- C012 Enforce economist password protection policy
The cost estimation is based on the yearly effort for deploying the policy by system administration.
[Included in Mitigation Set:](#) V

Entry Points:

- E002 The economist desktop application for updating rates

Attacker Types:

- K002 Insider

Tags:

- G004 Data
- G009 Software Modules

T006 Malicious hacker corrupts database by connecting to database server directly from internet

Description:

Damage: 7.2 % from total system assets

Probability: 0.82

Risk: Maximal: 5.9 % Current: 0.0 % Minimal: 0.0 %

Maximal Mitigation Available: 100.0 %

Threatened Assets:

- A001 The confidentiality of economists' personal information
Level of Damage: 100 %
- A003 The accuracy and integrity of the exchange rates data
Level of Damage: 90 %

Exploited Vulnerabilities:

- V001 The Web server and database server machines may be accessed through the internet. Anyone can reach the server machines by scanning the organization network from the internet. This vulnerability can be mitigated by controlling incoming network traffic.

Recommended Countermeasures:

- C001 Install firewall
The network is secured by using industry standard firewall, which is configured to block traffic from the internet to the local area network, excluding HTTP requests to Exchange Rates Web site. The cost of the implementation is the one time cost of the firewall purchase and deployment.
Included in Mitigation Set: V

Entry Points:

- E004 The database server

Attacker Types:

- K003 Hacker

Tags:

- G004 Data
- G005 Networking

Countermeasures by Theoretical Cost-Effectiveness

C001 Install firewall

Description:

The network is secured by using industry standard firewall, which is configured to block traffic from the internet to the local area network, excluding HTTP requests to Exchange Rates Web site. The cost of the implementation is the one time cost of the firewall purchase and deploy.

Cost Effectiveness: 5.5 % per 1,000 \$

Implementation Cost: 4,500 \$

Overall Mitigation: 24.8 % of total risk

Mitigated Vulnerabilities:

V001 The Web server and database server machines may be accessed through the internet

C008 Enforce policy of downloading and deployment of latest security patches for OS, database and Web server

Description:

The current security patches for all software infrastructures in the system should be maintained. The cost estimation is based on the yearly effort for deploying the patches by system administration.

Cost Effectiveness: 4.2 % per 1,000 \$

Implementation Cost: 5,000 \$

Overall Mitigation: 21.2 % of total risk

Mitigated Vulnerabilities:

V007 MS Server 2003 and IIS 6.0 have shortcomings that enable exploitation of OS resources via HTTP protocol

C013 Install anti-DoS appliance

Description:

The cost estimation is based on the one time expense for purchasing and deploying the appliance by system administration.

Cost Effectiveness: 4.1 % per 1,000 \$

Implementation Cost: 2,500 \$

Overall Mitigation: 10.2 % of total risk

Mitigated Vulnerabilities:

V011 Web servers are exposed to DoS attacks

C003 Enforce quality passwords policy for protecting each of the machines on the network

Description:

Network users should choose strong passwords that are hard to guess or discover by brute force means. The cost expresses the yearly effort of enforcing the password policy by system administration.

Cost Effectiveness: 2.9 % per 1,000 \$

Implementation Cost: 1,000 \$

Overall Mitigation: 2.9 % of total risk

Mitigated Vulnerabilities:

V002 The Web server and database server machines may be accessed through the LAN

C005 Database login accounts should be given the minimal rights that are necessary for their functionality

Description:

Web application account used for retrieving daily rates is assigned with read only permissions. Economist account is given update privileges only on rates data. DB administrator is the only account with full rights on the database that can access and modify data. The cost reflects administration effort.

Cost Effectiveness: 2.4 % per 1,000 \$

Implementation Cost: 3,500 \$

Overall Mitigation: 8.2 % of total risk

Mitigated Vulnerabilities:

V006 SQL server is prone to injection of malicious code via Web pages

V009 Unauthorized user of the economist application can enter the rates database

C018 Develop fraud detection mechanism

Description:

The fraud detection module will scan database and economist activity log.

Cost Effectiveness: 2.1 % per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 21.0 % of total risk

Mitigated Vulnerabilities:

V012 Economist can set currency rates and modify historical currency rates data

C017 Develop two-phase protocol for changing historical rates data that involves managerial personnel

Description:

Cost Effectiveness: 2.1 % per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 21.0 % of total risk

Mitigated Vulnerabilities:

V012 Economist can set currency rates and modify historical currency rates data

C016 Develop module for logging of economists' activities

Description:

The module will log all activities of logged-in users that use the economist application.

Cost Effectiveness: 2.1 % per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 21.0 % of total risk

Mitigated Vulnerabilities:

V012 Economist can set currency rates and modify historical currency rates data

C004 Use windows integrated authentication for database logins

Description:

This type of secured logging protocol requires the installation of Windows domain controller + Active Directory + backup domain controller. The cost expresses the one time expense for purchasing the software and the continuous deployment effort by system administration.

Cost Effectiveness: 1.5 % per 1,000 \$

Implementation Cost: 3,500 \$

Overall Mitigation: 5.3 % of total risk

Mitigated Vulnerabilities:

V004 The database passwords may be sniffed from the LAN when establishing connection to database server

V009 Unauthorized user of the economist application can enter the rates database

C012 Enforce economist password protection policy

Description:

The cost estimation is based on the yearly effort for deploying the policy by system administration.

Cost Effectiveness: 1.2 % per 1,000 \$

Implementation Cost: 2,000 \$

Overall Mitigation: 2.4 % of total risk

Mitigated Vulnerabilities:

V009 Unauthorized user of the economist application can enter the rates database

C020 Set severe punishments in law against insiders' economical crimes

Description:

Cost Effectiveness: 0.8 % per 1,000 \$

Implementation Cost: 25,000 \$

Overall Mitigation: 21.0 % of total risk

Mitigated Vulnerabilities:

V012 Economist can set currency rates and modify historical currency rates data

C006 Implement validation of input fields in rates web pages

Description:

For example: validate the input to the date field in the rates page. The cost expresses the one time effort for developing this software feature.

Cost Effectiveness: 0.6 % per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 5.8 % of total risk

Mitigated Vulnerabilities:

V006 SQL server is prone to injection of malicious code via Web pages

C007 Enforce data access via stored procedures with formal parameters content validation

Description:

Data in database should be manipulated only via stored procedures. The parameters of the stored procedures should be validate for their content before executing the stored procedure. The cost here is the one time effort for developing this software feature.

Cost Effectiveness: 0.6 % per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 5.8 % of total risk

Mitigated Vulnerabilities:

V006 SQL server is prone to injection of malicious code via Web pages

C009 Enforce security code review

Description:

Review all system's source codes according to 'secure code writing' industry standards. The cost here is the one time effort for implementing this software review.

Cost Effectiveness: 0.6 % per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 5.8 % of total risk

Mitigated Vulnerabilities:

V006 SQL server is prone to injection of malicious code via Web pages

C002 Physically protect access to local network wiring

Description:

If network is compromised, sensitive data could be viewed as a result of direct attacks on database server. The cost of the physically protection of the LAN is a one time expense.

Cost Effectiveness: 0.4 % per 1,000 \$

Implementation Cost: 7,000 \$

Overall Mitigation: 2.9 % of total risk

Mitigated Vulnerabilities:

V002 The Web server and database server machines may be accessed through the LAN

V004 The database passwords may be sniffed from the LAN when establishing connection to database server

C019 Security officer will have mandate to assure the personal integrity of economists

Description:

Cost Effectiveness: 0.3 % per 1,000 \$

Implementation Cost: 30,000 \$

Overall Mitigation: 9.0 % of total risk

Mitigated Vulnerabilities:

V013 Economist personal weaknesses may be exploited by hostile parties

C010 Economist application login should be bound with Windows login

Description:

The cost here is the one time effort for developing this software feature.

Cost Effectiveness: 0.2 % per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 2.4 % of total risk

Mitigated Vulnerabilities:

V009 Unauthorized user of the economist application can enter the rates database

C011 Implement validation of input fields in economist application

Description:

Data fields inputs should be validated before transmitted to database. The cost here is the one time effort for developing this software feature.

Cost Effectiveness: 0.% per 1,000 \$

Implementation Cost: 10,000 \$

Overall Mitigation: 0.% of total risk

Mitigated Vulnerabilities: None

Mitigation Plans by ROSI

Mitigation Plan: C008

Threats Mitigated by Mitigation Plan:

T007 Hacker uses HTTP requests to get access to OS resources of the Web server
Value at Risk: 152,507 \$ Mitigation Level: 82.0 %

Countermeasures in Mitigation Plan:

C008 Enforce policy of downloading and deployment of latest security patches for OS, database
Cost: 5,000 \$

Cost of Implementing Mitigation Plan: 5,000 \$

Return On Security Investment (ROSI): 2401.1 %

Mitigation Plan: C001, C013

Threats Mitigated by Mitigation Plan:

T005 Denial of Service attack on the web site
Value at Risk: 72,957 \$ Mitigation Level: 82.0 %
T006 Malicious hacker corrupts database by connecting to database server directly from internet
Value at Risk: 86,142 \$ Mitigation Level: 100.0 %

Countermeasures in Mitigation Plan:

C001 Install firewall
Cost: 4,500 \$
C013 Install anti-DoS appliance
Cost: 2,500 \$

Cost of Implementing Mitigation Plan: 7,000 \$

Return On Security Investment (ROSI): 1985.2 %

Mitigation Plan: C001

Threats Mitigated by Mitigation Plan:

T006 Malicious hacker corrupts database by connecting to database server directly from internet
Value at Risk: 86,142 \$ Mitigation Level: 100.0 %

Countermeasures in Mitigation Plan:

C001 Install firewall
Cost: 4,500 \$

Cost of Implementing Mitigation Plan: 4,500 \$

Return On Security Investment (ROSI): 1814.3 %

Mitigation Plan: C002, C003, C004

Threats Mitigated by Mitigation Plan:

T004 Malicious insider connects to database via LAN for corrupting and/or altering the data
Value at Risk: 16,848 \$ Mitigation Level: 100.0 %

Countermeasures in Mitigation Plan:

C002 Physically protect access to local network wiring
Cost: 7,000 \$
C003 Enforce quality passwords policy for protecting each of the machines on the network
Cost: 1,000 \$
C004 Use windows integrated authentication for database logins
Cost: 3,500 \$

Cost of Implementing Mitigation Plan: 11,500 \$

Return On Security Investment (ROSI): 46.5 %

Mitigation Plan: C016, C017, C018, C020

Threats Mitigated by Mitigation Plan:

T009 A malicious economist forges currency rates
Value at Risk: 141,226 \$ Mitigation Level: 50.0 %

Countermeasures in Mitigation Plan:

C016 Develop module for logging of economists' activities
Cost: 10,000 \$
C017 Develop two-phase protocol for changing historical rates data that involves managerial
Cost: 10,000 \$
C018 Develop fraud detection mechanism
Cost: 10,000 \$
C020 Set severe punishments in law against insiders' economical crimes
Cost: 25,000 \$

Cost of Implementing Mitigation Plan: 55,000 \$

Return On Security Investment (ROSI): 28.4 %

Mitigation Plan: C005, C006, C007, C009

Threats Mitigated by Mitigation Plan:

T001 Hacker corrupts database by injecting malicious SQL statements in input fields of the rates
Value at Risk: 34,135 \$ Mitigation Level: 100.0 %

Countermeasures in Mitigation Plan:

C005 Database login accounts should be given the minimal rights that are necessary for their
Cost: 3,500 \$
C006 Implement validation of input fields in rates web pages
Cost: 10,000 \$
C007 Enforce data access via stored procedures with formal parameters content validation

Cost: 10,000 \$
C009 Enforce security code review
Cost: 10,000 \$

Cost of Implementing Mitigation Plan: 33,500 \$

Return On Security Investment (ROSI): 1.9 %

Mitigation Plan: C004, C005, C010, C012

Threats Mitigated by Mitigation Plan:

T002 Insider corrupts database by injecting malicious SQL statements in input fields of the
Value at Risk: 14,357 \$ Mitigation Level: 100.0 %

Countermeasures in Mitigation Plan:

C004 Use windows integrated authentication for database logins
Cost: 3,500 \$
C005 Database login accounts should be given the minimal rights that are necessary for their
Cost: 3,500 \$
C010 Economist application login should be bound with Windows login
Cost: 10,000 \$
C012 Enforce economist password protection policy
Cost: 2,000 \$

Cost of Implementing Mitigation Plan: 19,000 \$

Return On Security Investment (ROSI): -24.4 %

Mitigation Plan: C016, C017, C018, C019, C020

Threats Mitigated by Mitigation Plan:

T010 Hostile countries may manipulate currency rates by recruiting economists
Value at Risk: 70,613 \$ Mitigation Level: 75.0 %

Countermeasures in Mitigation Plan:

C016 Develop module for logging of economists' activities
Cost: 10,000 \$
C017 Develop two-phase protocol for changing historical rates data that involves managerial
Cost: 10,000 \$
C018 Develop fraud detection mechanism
Cost: 10,000 \$
C019 Security officer will have mandate to assure the personal integrity of economists
Cost: 30,000 \$
C020 Set severe punishments in law against insiders' economical crimes
Cost: 25,000 \$

Cost of Implementing Mitigation Plan: 85,000 \$

Return On Security Investment (ROSI): -37.7 %

Optimized Risk Reduction Plan

This report presents a recommended sequence of mitigation steps that will reduce the system's risk to a given target level in the most cost-effective way. Each step in the plan is comprised of countermeasures that should be implemented in order to achieve the step's contribution to risk reduction.

System's Risk Status

(in % of total system assets value)

Maximal risk	40.2 %
Minimal risk	8.8 %
Current risk	25.8 %

Step # : 1

List of countermeasures that should be implemented in this step:

C013 Install anti-DoS appliance

Countermeasure Implementation Cost:	2,500 \$
Accumulated Cost of Step:	2,500 \$
Accumulated Cost of Plan:	2,500 \$

Risk remaining after implementation of step's countermeasures: **21.7 %**

Step # : 2

List of countermeasures that should be implemented in this step:

C003 Enforce quality passwords policy for protecting each of the machines on the network

Countermeasure Implementation Cost:	1,000 \$
Accumulated Cost of Step:	1,000 \$
Accumulated Cost of Plan:	3,500 \$

C002 Physically protect access to local network wiring

Countermeasure Implementation Cost:	7,000 \$
Accumulated Cost of Step:	8,000 \$
Accumulated Cost of Plan:	10,500 \$

Risk remaining after implementation of step's countermeasures: **20.6 %**

Step # : 3

List of countermeasures that should be implemented in this step:

C020 Set severe punishments in law against insiders economical crimes

Countermeasure Implementation Cost:	25,000 \$
Accumulated Cost of Step:	25,000 \$
Accumulated Cost of Plan:	35,500 \$

C019 Security officer will have mandate to assure the personal integrity of economists

Countermeasure Implementation Cost:	30,000 \$
Accumulated Cost of Step:	55,000 \$
Accumulated Cost of Plan:	65,500 \$

C018 Develop fraud detection mechanism

Countermeasure Implementation Cost:	10,000 \$
Accumulated Cost of Step:	65,000 \$
Accumulated Cost of Plan:	75,500 \$

C017 Develop two-phase protocol for changing historical rates data that involves managerial personnel

Countermeasure Implementation Cost:	10,000 \$
Accumulated Cost of Step:	75,000 \$
Accumulated Cost of Plan:	85,500 \$

C016 Develop module for logging of economists' activities

Countermeasure Implementation Cost:	10,000 \$
Accumulated Cost of Step:	85,000 \$
Accumulated Cost of Plan:	95,500 \$

Risk remaining after implementation of step's countermeasures: 12.1 %

Step # : 4

List of countermeasures that should be implemented in this step:

C012 Enforce economist password protection policy

Countermeasure Implementation Cost:	2,000 \$
Accumulated Cost of Step:	2,000 \$
Accumulated Cost of Plan:	97,500 \$

C010 Economist application login should be bound with Windows login

Countermeasure Implementation Cost:	10,000 \$
Accumulated Cost of Step:	12,000 \$
Accumulated Cost of Plan:	107,500 \$

Risk remaining after implementation of step's countermeasures: **11.1** %

Step # : 5

List of countermeasures that should be implemented in this step:

C009 Enforce security code review

Countermeasure Implementation Cost:	10,000 \$
Accumulated Cost of Step:	10,000 \$
Accumulated Cost of Plan:	117,500 \$

C007 Enforce data access via stored procedures with formal parameters content validation

Countermeasure Implementation Cost:	10,000 \$
Accumulated Cost of Step:	20,000 \$
Accumulated Cost of Plan:	127,500 \$

C006 Implement validation of input fields in rates web pages

Countermeasure Implementation Cost:	10,000 \$
Accumulated Cost of Step:	30,000 \$
Accumulated Cost of Plan:	137,500 \$

Risk remaining after implementation of step's countermeasures: **8.8** %