Appendix G

Sample Threat Checklist

For years I have worked to establish a sample list of threats that could be used by risk management professionals to expedite the risk assessment process. A few years ago when I was doing a class in Brazil a student gave me a URL that has helped the threat identification process. A German organization, IT-Grundschutz, has established two important lists for the risk management professional. The organization's aim is to achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements and that can also serve as the basis for IT systems and applications requiring a high degree of protection. This is achieved through the appropriate application of organizational, personnel, infrastructural, and technical standard security safeguards.

The threats catalog contains 426 pages of threats in detail. The threats are divided into five categories:

Threat Category	*Number of Threats*
Force majeure	15
Organizational shortcomings	101
Human failure	76
Technical threat	52
Deliberate acts	126

The URL to access the list of threats (Table G.2) is http//www.bsi/English/gshb/index.htm.

Table G.1 Sample Threat Checklist

Threat	*Applicable (Yes/No)*
Integrity	
Data stream could be intercepted.	
Faulty programming could (inadvertently) modify data.	
Written or electronic copies of reports could be diverted to unauthorized or unintended persons.	
Data could be entered incorrectly.	
Intentional incorrect data entry.	
Use of outdated programs could compromise integrity of information.	
Faulty hardware could result in inaccurate data entry and analysis.	
Third parties could modify data.	
Files could be accidentally deleted.	
Hackers could change data.	
Internal users could launch unauthorized programs to access and or modify bank data.	
Reports could be falsified.	
Internal theft of information by employees could be modified and used later.	
Network sniffing could intercept user passwords and allow unauthorized modification of information.	
Information could be outdated.	
Hackers could obtain unauthorized access into network to corrupt system resources.	
Physical intrusion by unauthorized persons.	
Documents could be falsified to appear as official company documents.	
Unauthorized or fictitious sales could be approved.	
Information could be misinterpreted due to language barriers.	
Fraudulent programming could impact data integrity, e.g., hidden hooks.	
Computer viruses could modify data.	
Information could be misdirected.	
Transactions could be intentionally not run or misrouted.	
Newer or upgraded software could cause corruption of documents or files.	

Table G.1 (continued) Sample Threat Checklist

Threat	*Applicable (Yes/No)*
Non-standard procedures could cause misinterpretation of information.	
Unauthorized persons may use an unattended workstation.	
Information to and from third parties could be corrupted in transmission.	
Account information may be shared.	
A power failure could corrupt information.	
Information could be submitted in a vague or misleading manner.	
Someone could impersonate a customer to corrupt records (identity theft).	
Information could be taken outside the company.	
Integrity of information could be compromised due to decay of information media.	
Someone could impersonate an employee to corrupt information.	
A terminated employee could intentionally corrupt information.	
Company could be targeted for system hacking by a dissatisfied customer.	
A default username and password for a network device could be exploited to gain access to system resources.	
Confidentiality	
Insecure e-mail could contain confidential information.	
Internal theft of information.	
Employee is not able to verify the identity of a client, e.g., phone masquerading.	
Confidential information is left in plain view on a desk.	
Social discussions outside the office could result in disclosure of sensitive information.	
Information could be salvaged by unauthorized persons from dumpsters or other waste receptacles.	
Information sent to third parties may be misused.	
Unattended computer could give unauthorized access to files.	
Passwords may not be required for all workstations.	
Mailing two or more different customer statements/documents in one envelope.	
Unauthorized people in confidential or restricted areas.	

continued

Table G.1 (continued) Sample Threat Checklist

Threat	*Applicable (Yes/No)*
Confidential information may be left on the fax or copy machine granting unauthorized viewing of documents.	
Fraudulent or misrepresentation of individuals in phone conversations.	
Response to a fax request without verification.	
Documents sent out for authorization could be forged and then returned.	
Unauthorized access to information by viewing documents over the shoulder of an employee (shoulder surfing).	
Documents could be excessively duplicated.	
Employee passwords could be shared.	
Interoffice messengers may handle confidential information.	
Employee and messenger relationships could exchange sensitive or confidential information.	
Unauthorized disclosure of information by third parties.	
Not adequately destroying electronic media may leave information available to unauthorized persons.	
Inadequate firewall configuration could inadvertently allow disclosure of information.	
Actual client information could be used on templates causing disclosure of sensitive information.	
Employees may be overheard discussing confidential information outside the office.	
Documents could be inadvertently delivered to wrong person.	
Holding phone conversations when unable to verify identity.	
Company could be subjected to electronic eavesdropping.	
Terminated employees may be able to access the building or information.	
Cleaning crews may see confidential information.	
Rubbish could contain confidential information.	
Employees may not follow the dual control procedures.	
Temporary or new employees may be insufficiently trained.	
Restricted areas may be accessed by visitors.	
Use of the speaker phone may violate confidentiality.	
Information and files may be inappropriately accessed on company's systems.	

Table G.1 (continued) Sample Threat Checklist

Threat	*Applicable (Yes/No)*
Data stored off site could be compromised.	
Employees may install illegal or unauthorized software.	
Consultants or other contracted help may view confidential information.	
Availability	
Files stored in personal directories may not be available to other employees when needed.	
Hardware failures could impact the availability of company resources.	
A failure in the data circuit could prohibit system access.	
"Acts of God": tornado, tsunami, hurricane.	
Upgrades in the software may prohibit access.	
Company system could be unavailable or down.	
Eating and drinking at a workstation could cause keyboard failure.	
An undersecured work area could jeopardize the confidentiality of customer information.	
A power failure could interrupt employee access.	
Software upgrades could affect other programs.	
Expired user access and/or insufficient employee training could disrupt the computer system.	
Availability of PCs shared by multiple users may be inadequate.	
Vendor or supplier support personnel may be unavailable due to the time zone differences.	
A communication failure could disrupt business operations.	
Employees may have incorrect or inappropriate file access.	
If a person is out (sick/absent) some critical files cannot be accessed.	
Issues with third-party support to fix problems would give access to confidential information.	
An absent person or tools could prevent backup if not available.	
Company could be subject to bombs or other acts of terrorism.	
Theft of equipment or other information.	
Insufficient cross-training of critical procedures could impact Fred's business processes.	
Availability of information resources controlled by third party could impact business processes.	

continued

Table G.1 (continued) Sample Threat Checklist

Threat	*Applicable (Yes/No)*
Damaged or altered storage or hardware media.	
Not all workstations have all programs loaded.	
Users could lose or misplace files.	
In today's environment there is a risk of man-made threats.	
Geography and getting materials in, due to distance.	
Vandalism and sabotage could be attempted to the network.	
Number of software licenses could be Insufficient.	
Insufficient personnel resources could impact business processes	
A computer virus could be introduced via e-mail or disk.	
Denial-of-service attacks from malicious Internet users outside of Fred's.	
Employee causes a document to be inaccessible temporarily due to human error.	
Natural threat	
Electrical storm	
Ice storm	
Snowstorm/blizzard	
Major landslide	
Mudslide	
Tsunami	
Tornado	
Hurricane/typhoon	
High winds (70+ mph)	
Tropical storm	
Tidal flooding	
Seasonal flooding	
Local flooding	
Upstream dam /reservoir failure	
Sandstorm	
Volcanic activity	
Earthquake (2–4 on Richter scale)	
Earthquake (5 or more on Richter scale)	
Epidemic	
Human — Accidental	

Table G.1 (continued) Sample Threat Checklist

Threat	*Applicable (Yes/No)*
Fire: Internal–minor	
Fire: Internal–major	
Fire: Internal–catastrophic	
Fire: External	
Accidental explosion — on site	
Accidental explosion — off site	
Aircraft crash	
Train crash	
Derailment	
Auto/truck crash at site	
Human error — maintenance	
Human error — operational	
Human error — programming	
Human error — users	
Toxic contamination	
Medical emergency	
Loss of key staff	
Human — deliberate	
Environmental	
Power flux	
Power outage — internal	
Power outage — external	
Water leak/plumbing failure	
HVAC failure	
Temperature inadequacy	
Telecommunications failure	
Toxic contamination	

Table G.2 Natural Security Threats List

Threat	*Definition*
1. Terrorism	This issue concerns foreign power–sponsored or foreign power–coordinated activities that: ■ Involve violent acts. ■ Appear to be intended to intimidate or coerce. ■ Transcend national boundaries.
2. Espionage	Foreign power–sponsored or foreign power–coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, which involves the identification, targeting, and collection of U.S. national defense information.
3. Proliferation	Foreign power–sponsored or foreign power–coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments or persons, which involves: ■ The proliferation of weapons of mass destruction to include chemical, biological, or nuclear weapons, and delivery systems of those weapons of mass destruction; or ■ The proliferation of advanced conventional weapons.
4. Economic espionage	Foreign power–sponsored or foreign power–coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, which involves: ■ The unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information, or critical technologies; or ■ The unlawful or clandestine targeting or influencing of sensitive economic policy decisions.
5. Targeting the national information infrastructure	Foreign power–sponsored or foreign power–coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, which involves the targeting of facilities, personnel, information, or computer, cable, satellite, or telecommunications systems which are associated with the national information infrastructure. Proscribed intelligence activities include:

Table G.2 (continued) Natural Security Threats List

Threat	*Definition*
	■ Denial or disruption of computer, cable, satellite, or telecommunications services; ■ Unauthorized monitoring of computer, cable, satellite, or telecommunications systems; ■ Unauthorized disclosure of proprietary or classified information stored within or communicated through computer, cable, satellite, or telecommunications systems; ■ Unauthorized modification or destruction of computer programming codes, computer network databases, stored information, or computer capabilities; or ■ Manipulation of computer, cable, satellite, or telecommunications services resulting in fraud, financial loss, or other federal criminal violations.
6. Targeting the U.S. government	Foreign power–sponsored or foreign power–coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, which involves the targeting of government programs, information, or facilities, or the targeting or personnel of: ■ The U.S. intelligence community; ■ The U.S. foreign affairs, or economic affairs community; or ■ The U.S. defense establishment and related activities of national preparedness.
7. Perception management	Foreign power–sponsored or foreign power–coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, which involves manipulating information, communicating false information, or propagating deceptive information and communications designed to distort the perception of the public (domestically or internationally) or of U.S. government officials regarding U.S. policies, ranging from foreign policy to economic strategies.
8. Foreign intelligence activities	Foreign power–sponsored or foreign power–coordinated intelligence activity conducted in the United States, or directed against the U.S. government, or U.S. corporations, establishments, or persons, that is not described by or included in the other issue threats.

Source: http://www.ntc.doe.gov/cita/CI_Awareness_Guide/T1threat/Nstl.htm (Department of Energy National Training Center).