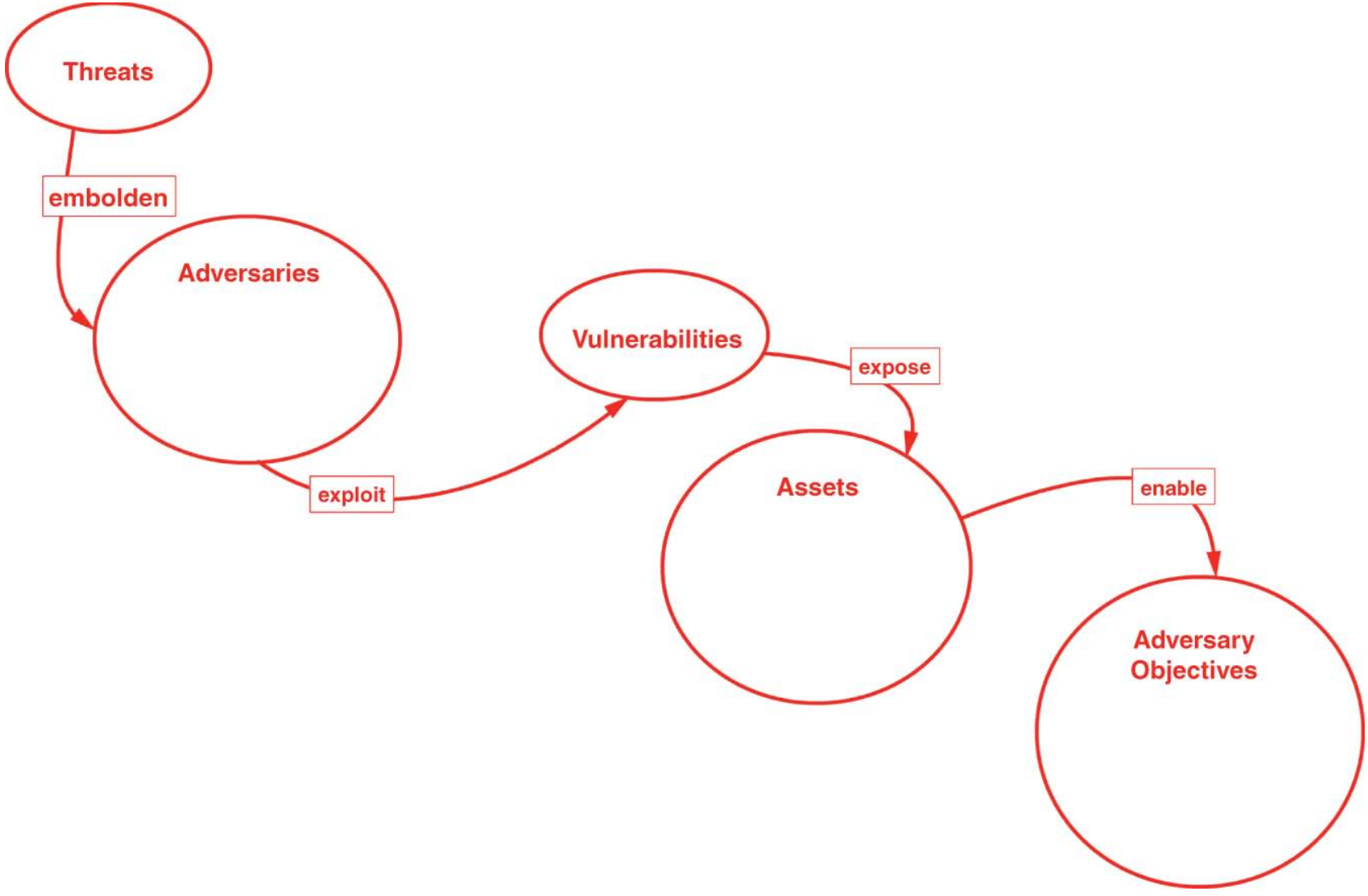
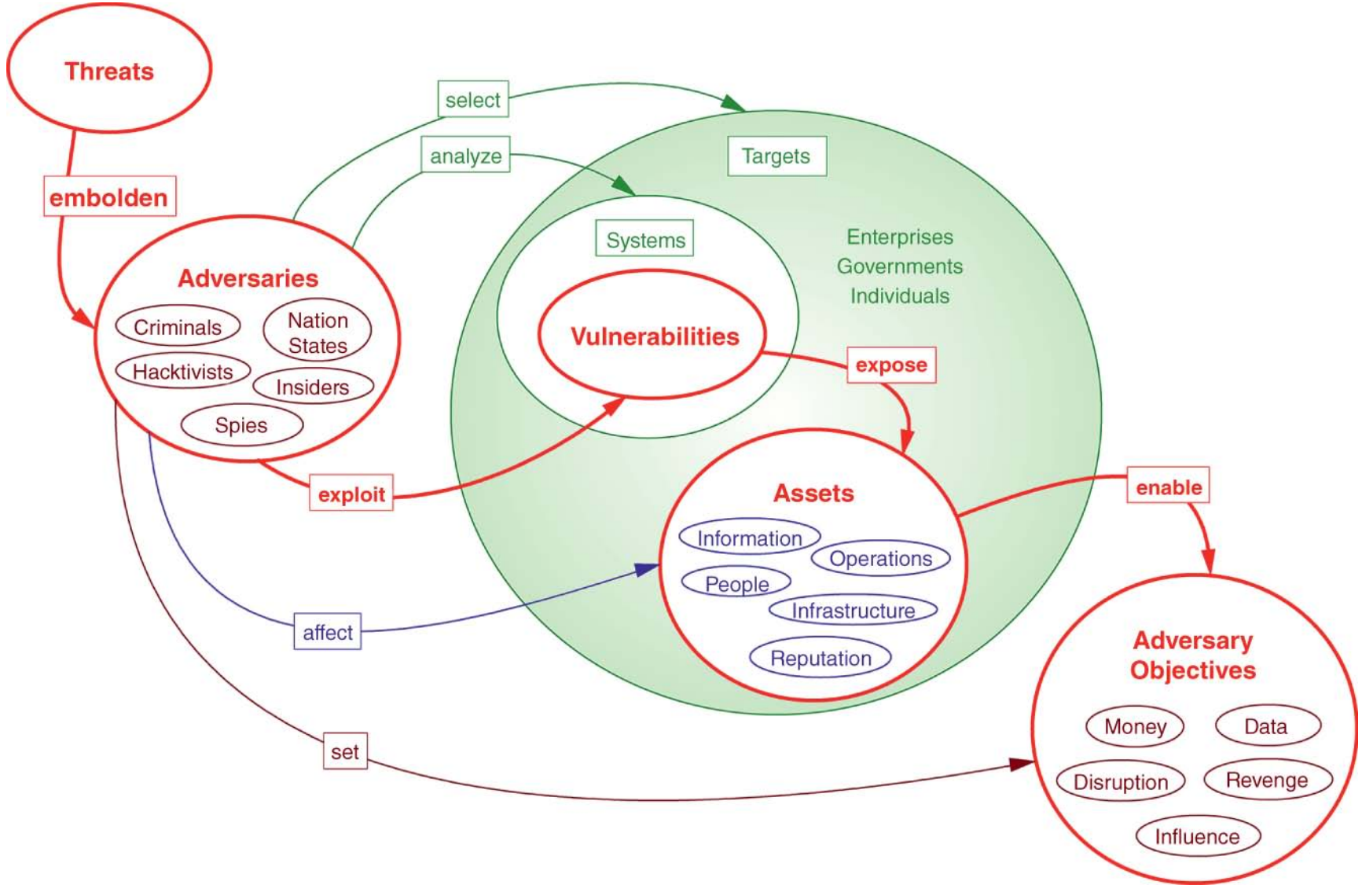


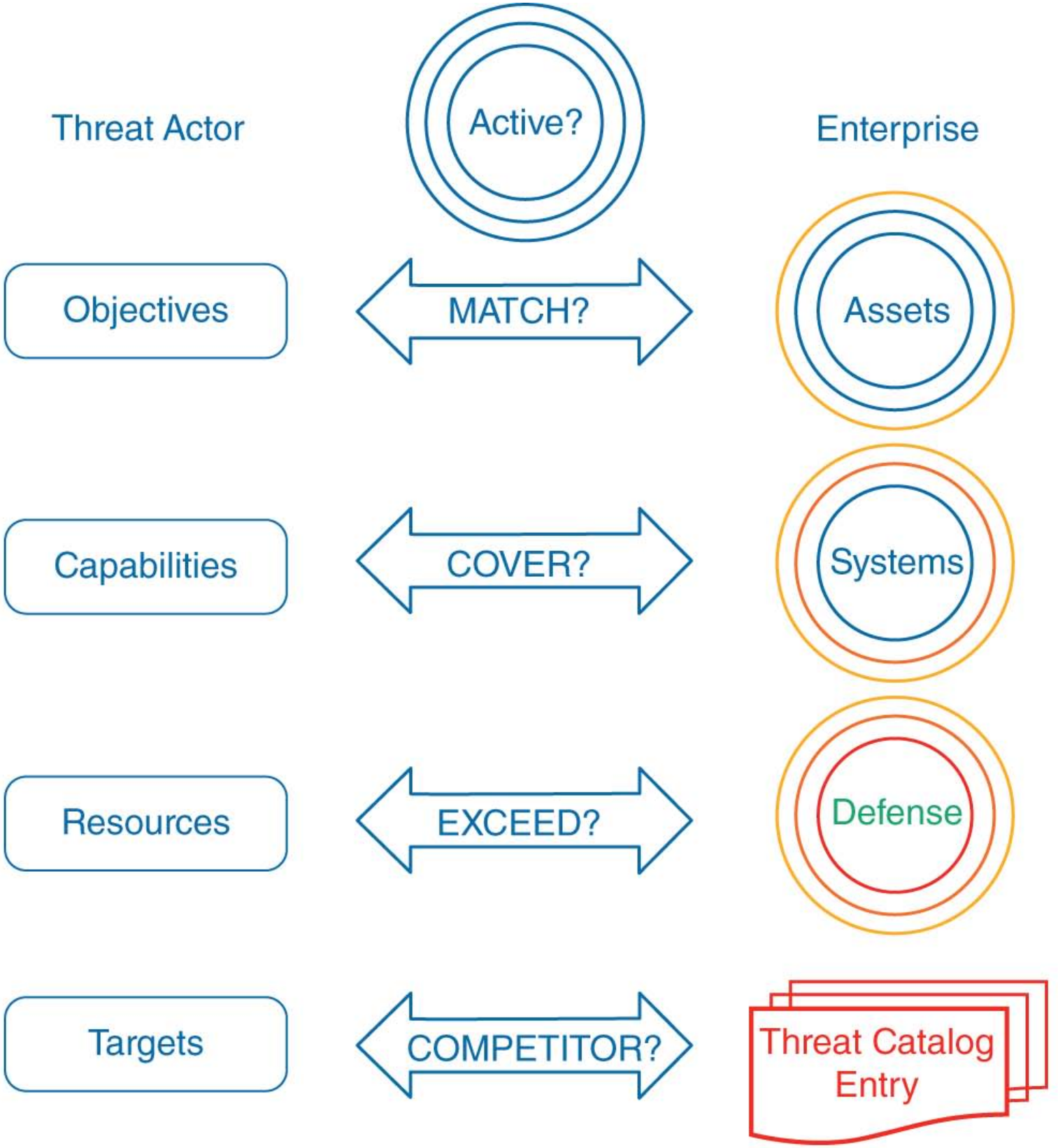
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.1



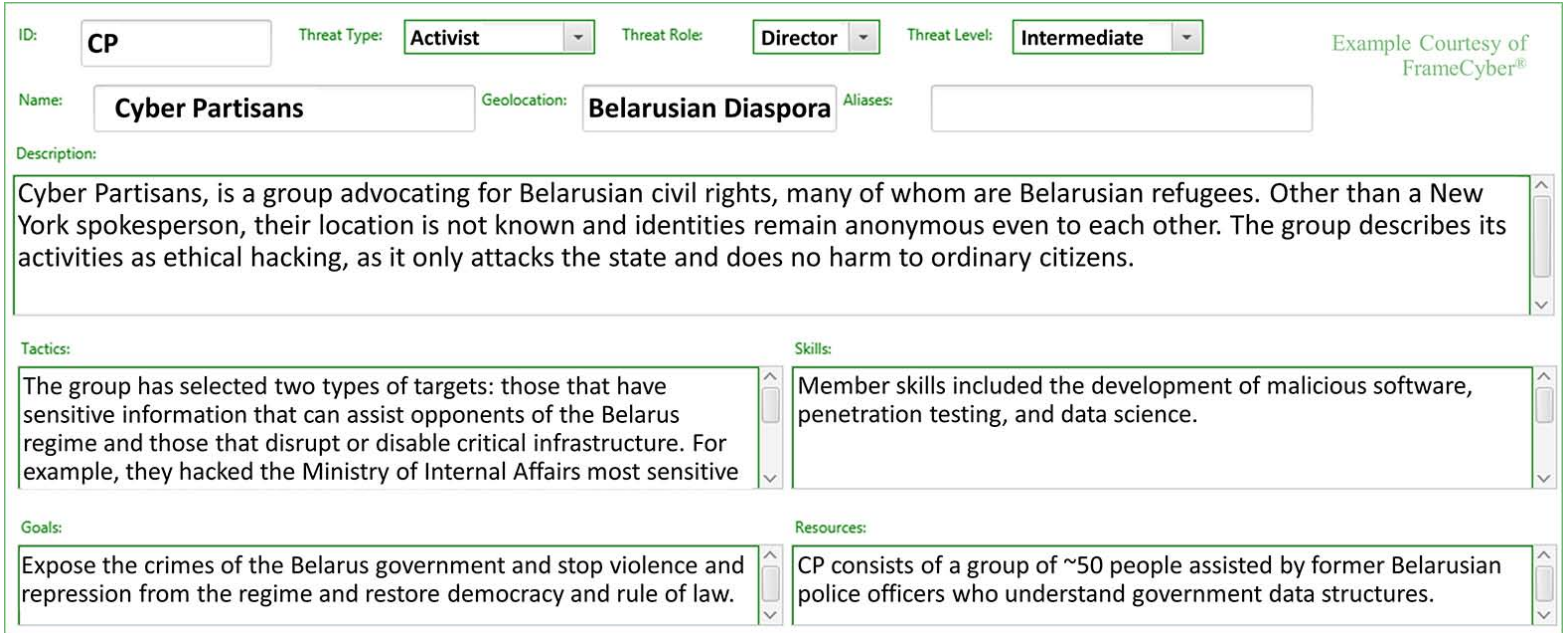
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.2

Threat Actor Type	Objective
Activist/Hacktivist	Make a political statement (Anonymous); voting systems
Competitor	Trade secrets, competitive analysis, or disruption of service
Criminal	Profit; anything they can monetize for cash
Crime-syndicate	Organized crime as a technology business
Hacker	Hacking for thrill or challenge
Insider-accidental	Unintentionally exposes the organization to harm
Insider-disgruntled	Financial gain; personal benefits for retaliation or revenge
Nation-state	World supremacy
Sensationalist	Embarrassment and brand damage
Spy	Cyber espionage
Terrorist	Telecom, energy grid, government defenses
Other, e.g. Lone Wolf	Cybercrime-as-a-service model is furthering the reach of solo actors.

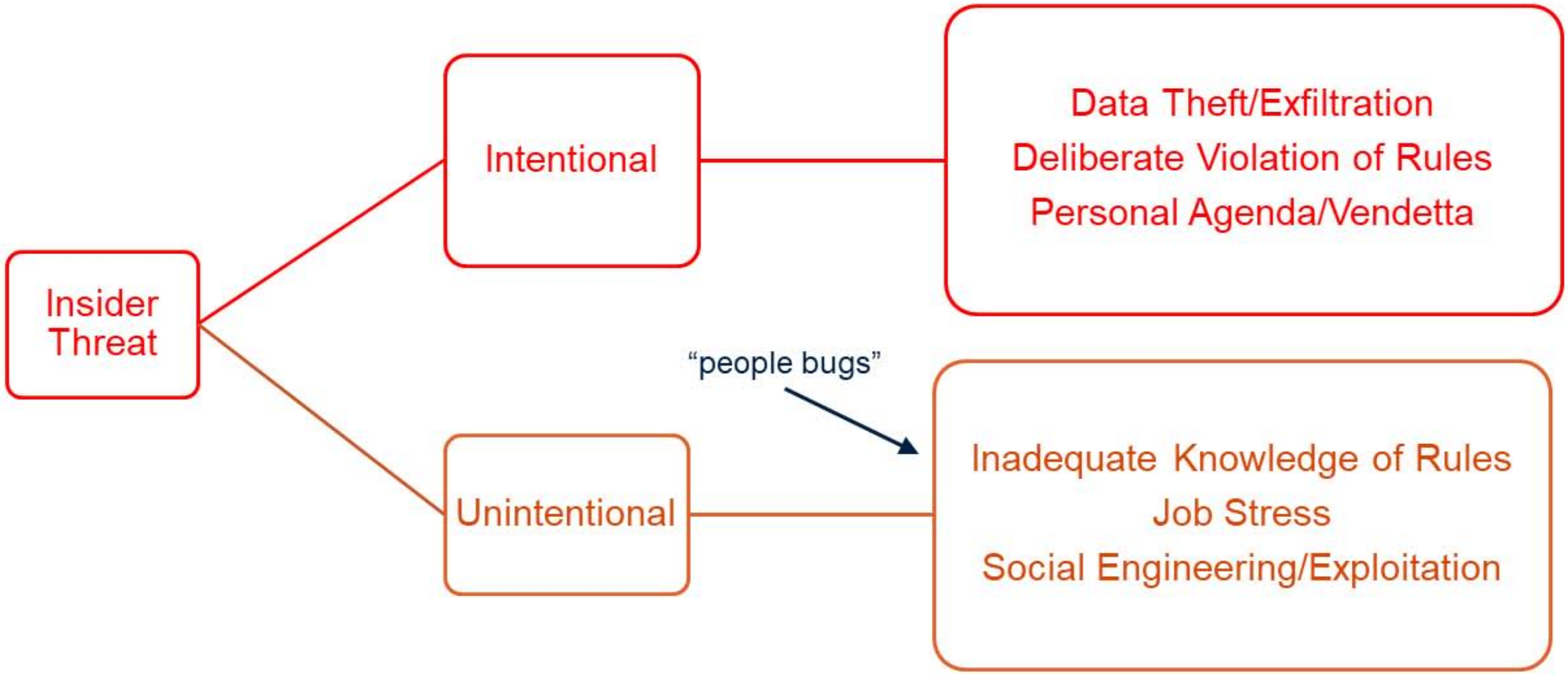
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.3



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.4



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.5



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.6

NBCDFW LOCAL WEATHER RESPONDS INVESTIGATIO

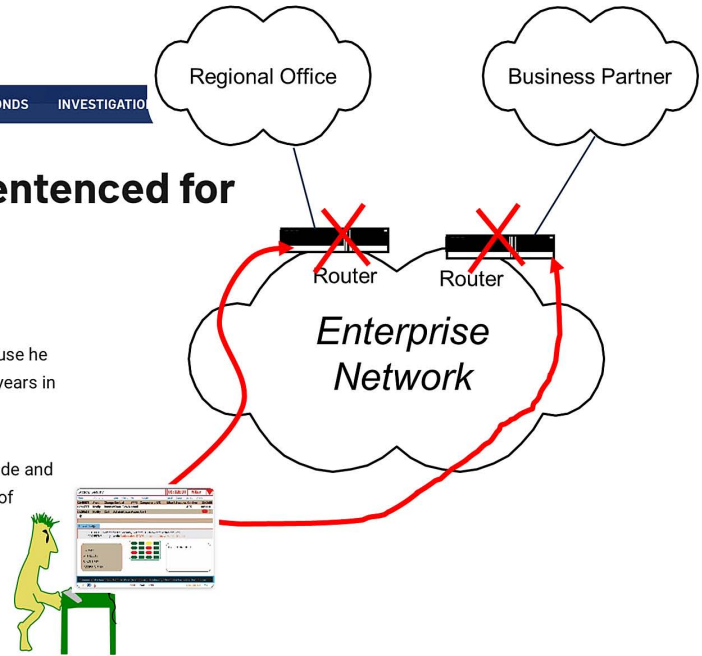
DALLAS

Dallas Citibank Worker Sentenced for Computer Sabotage

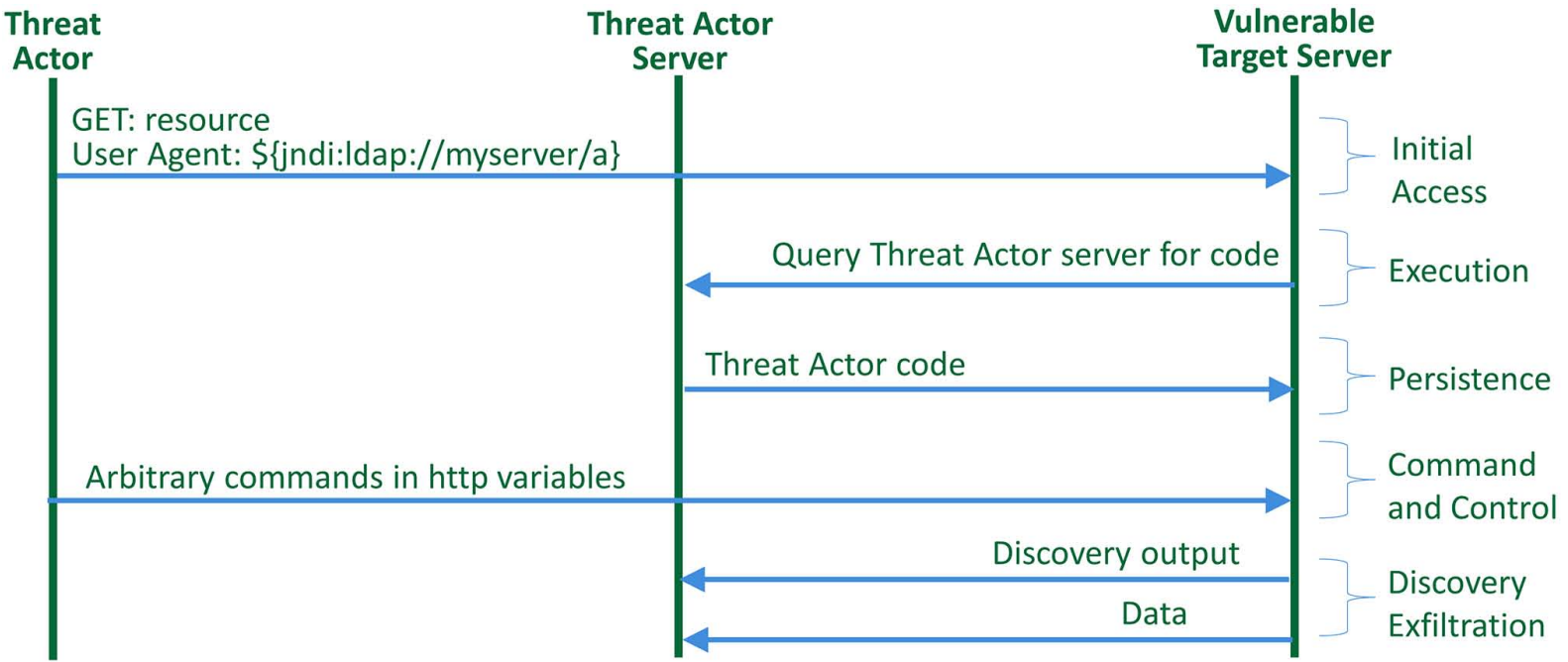
Published July 26, 2016 • Updated on July 26, 2016 at 9:15 am

An employee who sabotaged Citibank's computer system because he believed he was about to be fired was sentenced to nearly two years in prison.

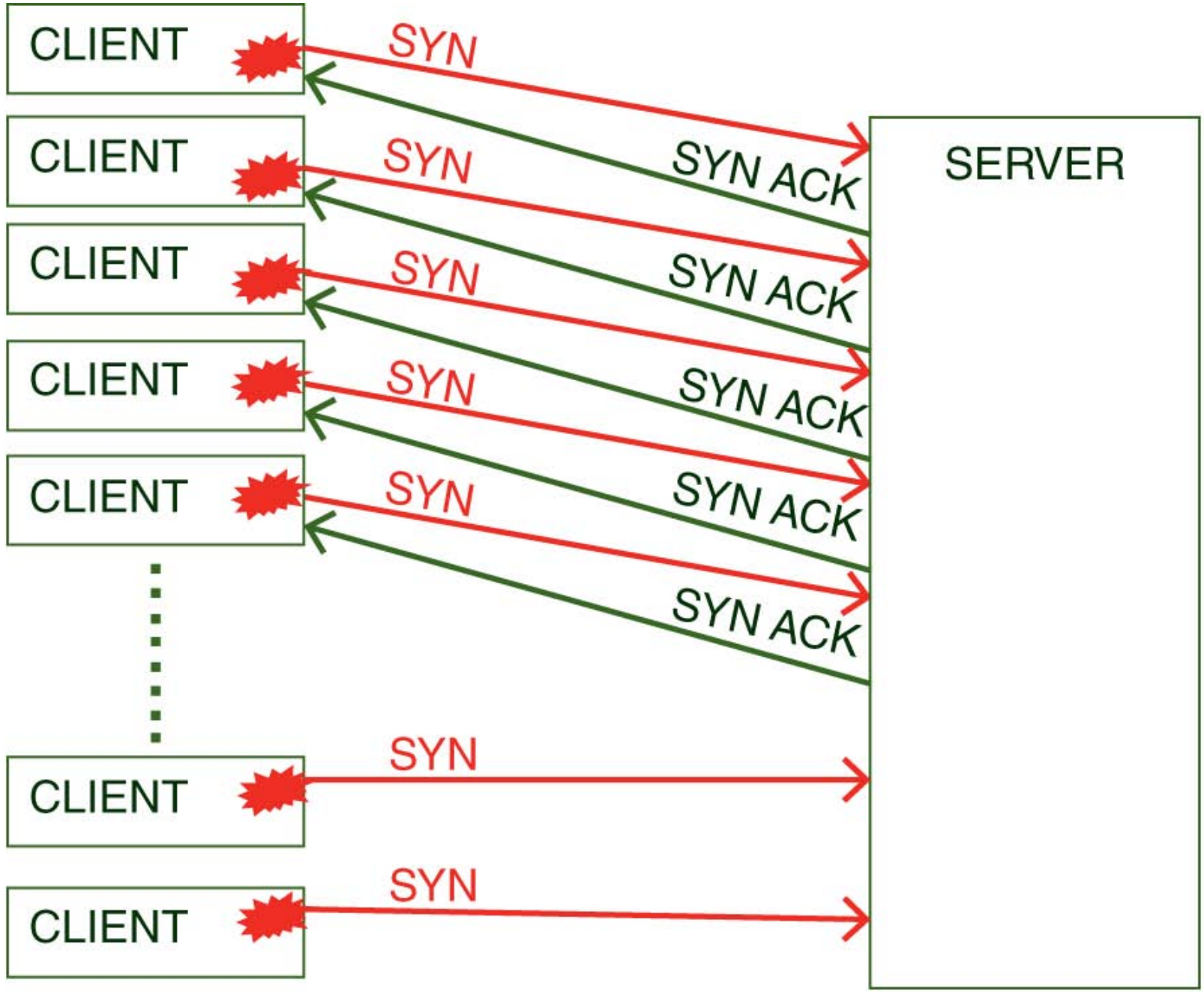
Investigators said Lennon Ray Brown of Dallas transmitted a code and command in 2013 leading to loss of connectivity to 90 percent of Citibank networks in North America.



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.7

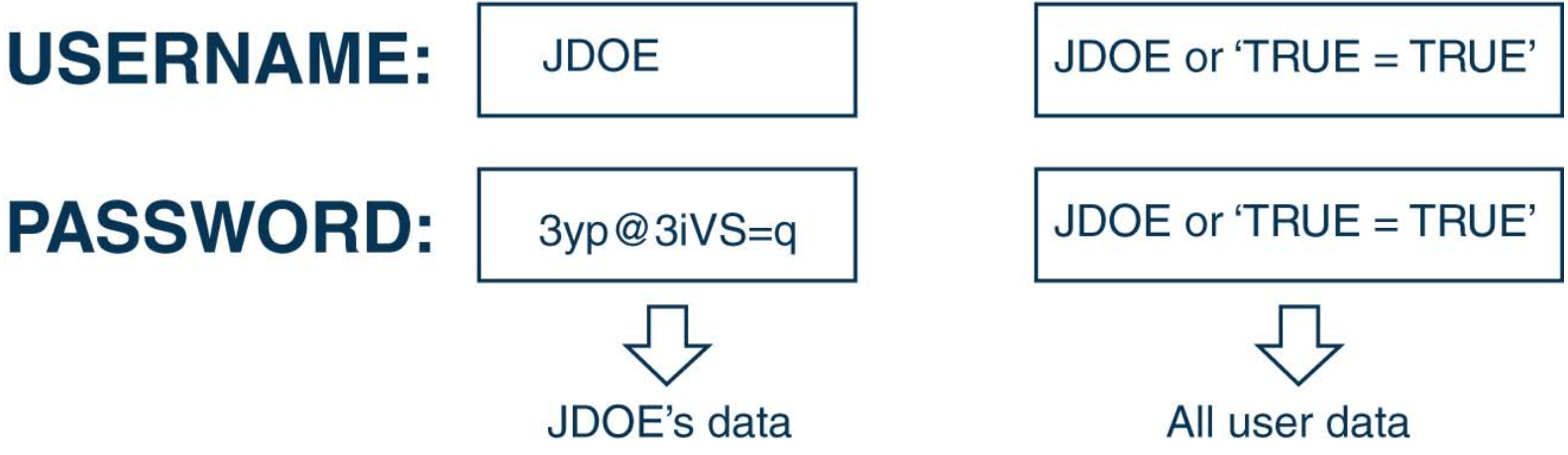


Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.8

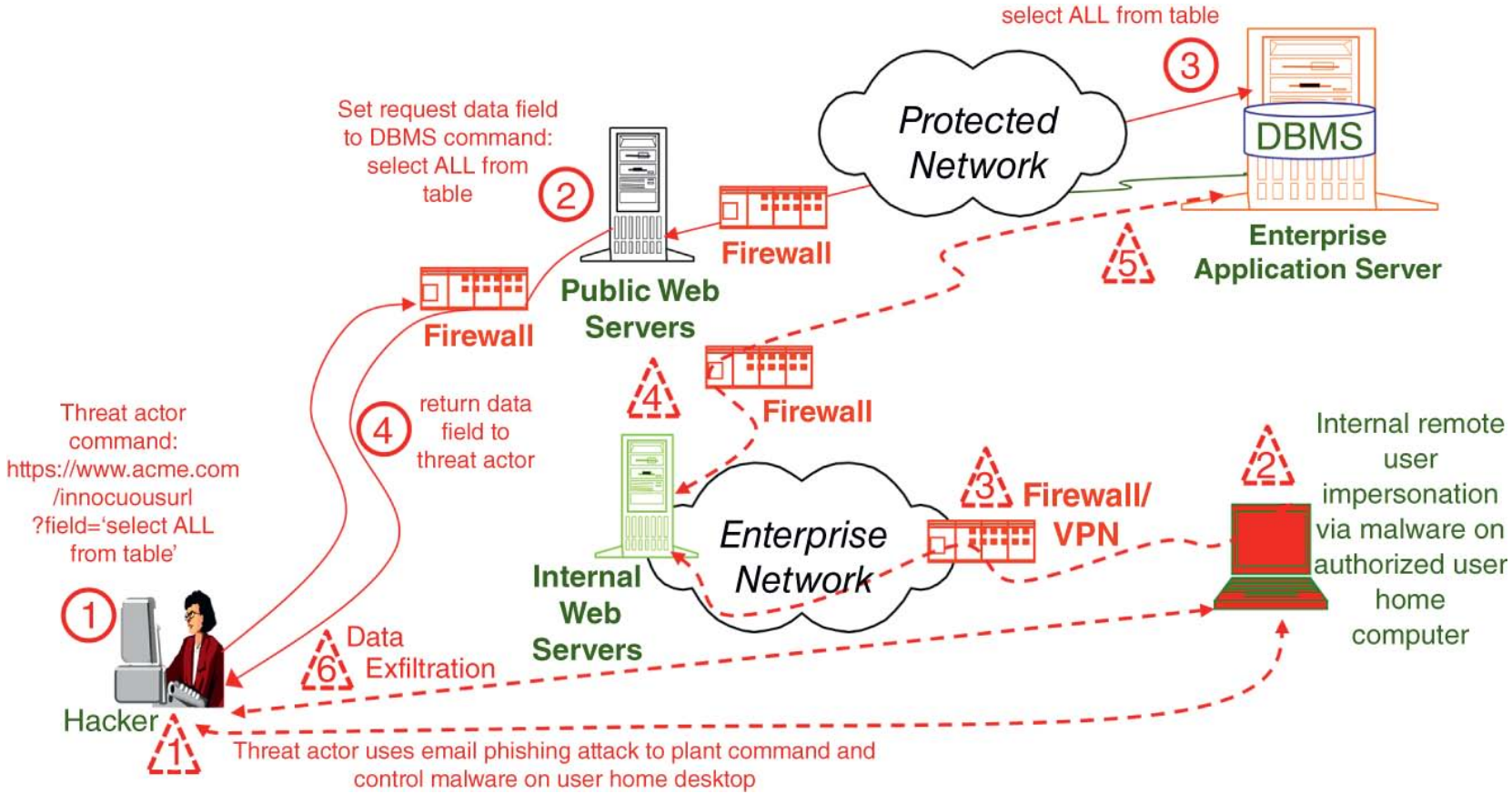


Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.9

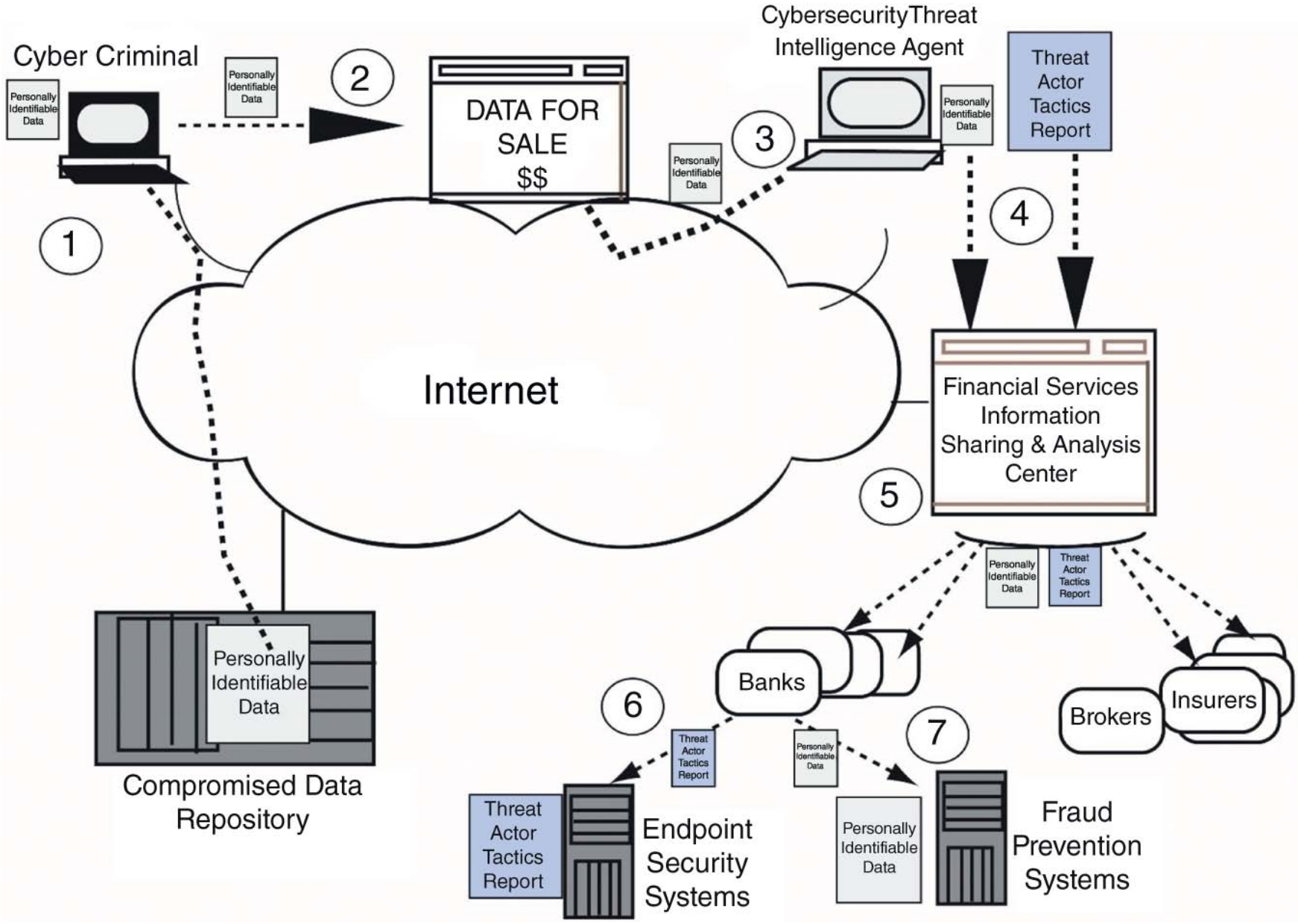
```
login = username_field_contents
pwd = password_field_contents
user_data = select user from CustomerData where (user.name = login) and (user.password = pwd)
display user_data
```



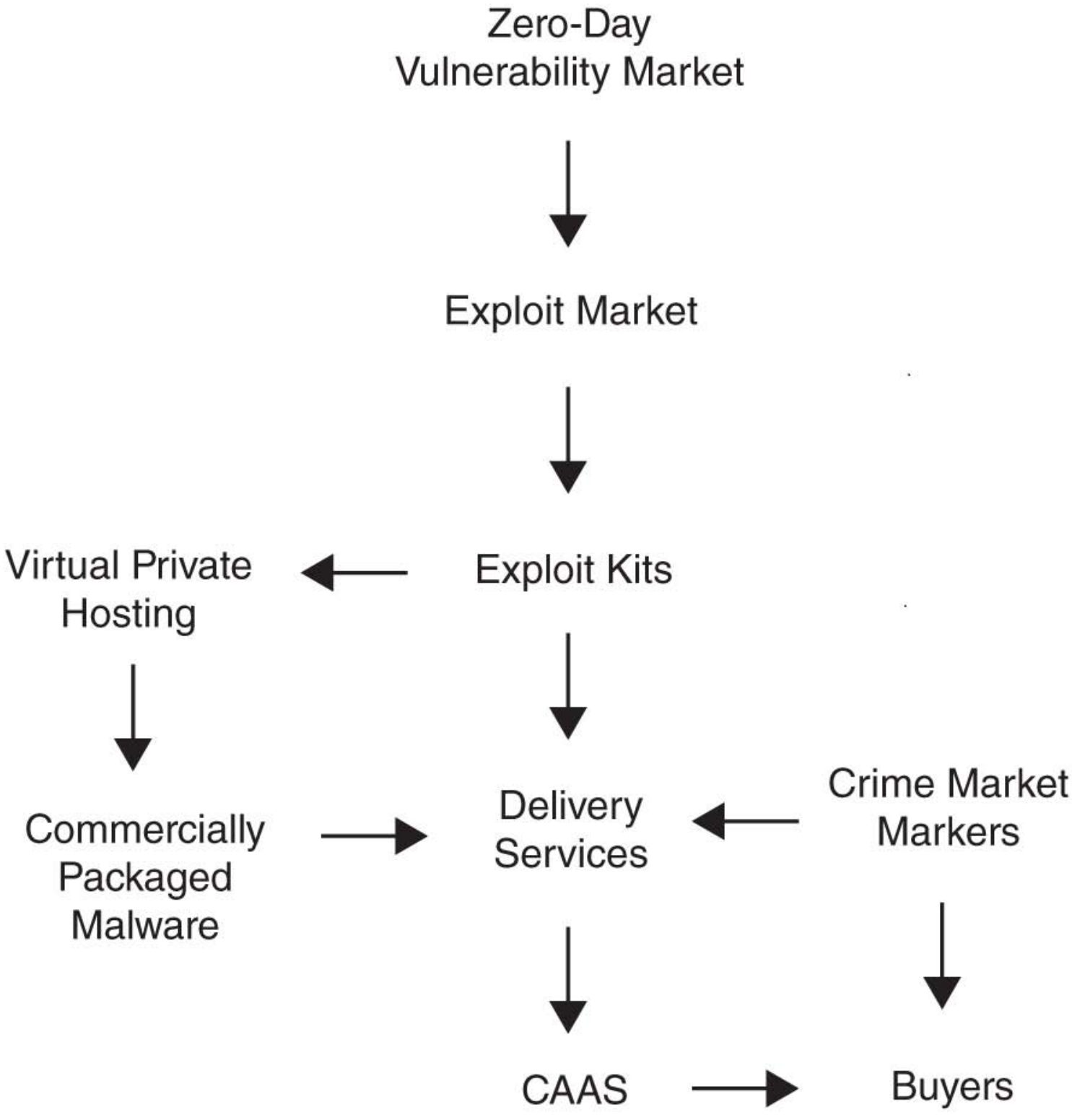
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.10



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.11



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.12



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.13

Reconnaissance	Gather information to plan future operations.
Resource Development	Establish resources to support operations.
Initial Access	Access target system or network.
Execution	Run malicious code on target system.
Persistence	Maintain a foothold within target systems.
Privilege Escalation	Gain higher-level permissions.
Defense Evasion	Avoid being detected.
Credential Access	Steal account names and passwords.
Discovery	Map out target environment.
Lateral Movement	Move through target environment.
Collection	Gather data of interest to goal.
Command and Control	Communicate with compromised systems to control them.
Exfiltration	Steal data.
Impact	Manipulate, interrupt, or destroy target systems and data.

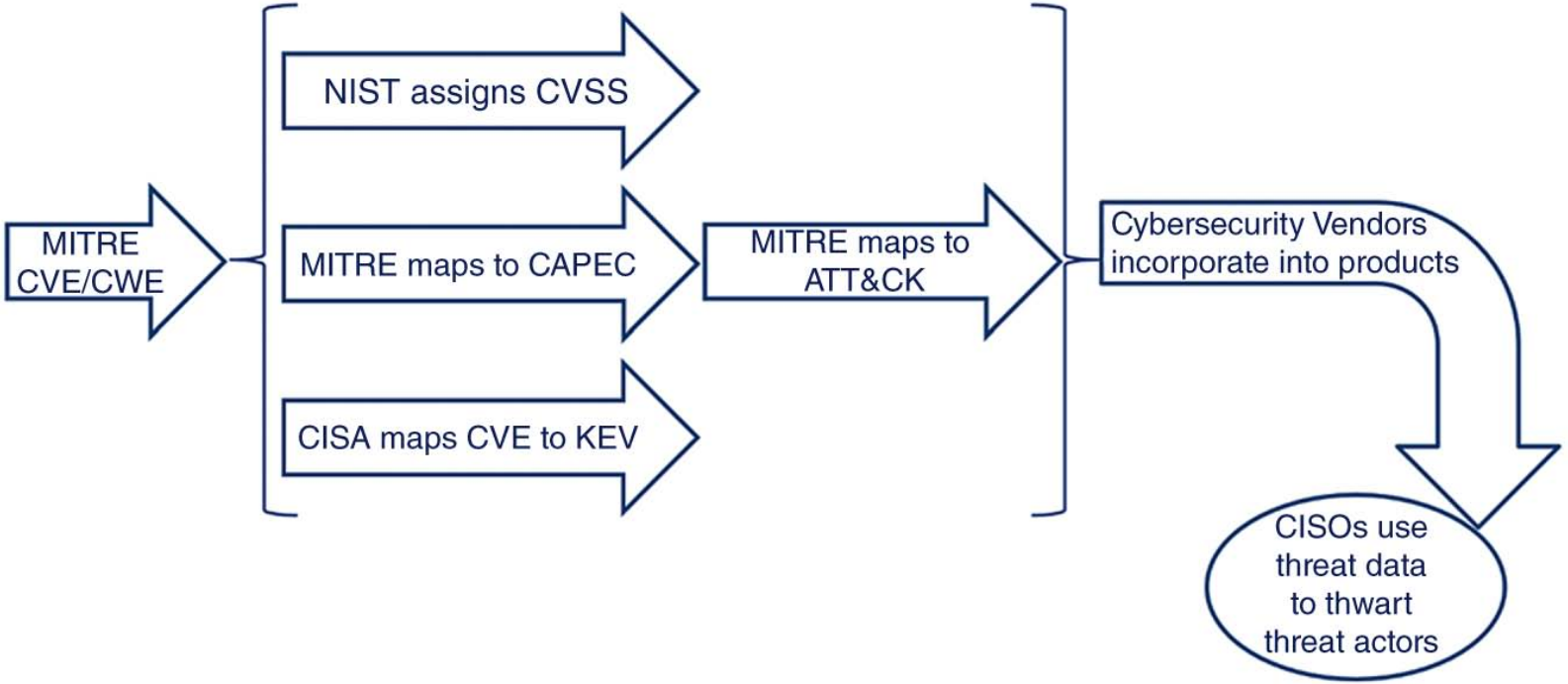
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.14

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.15

Table 1 - Vulnerability Tower of Babel, 1998

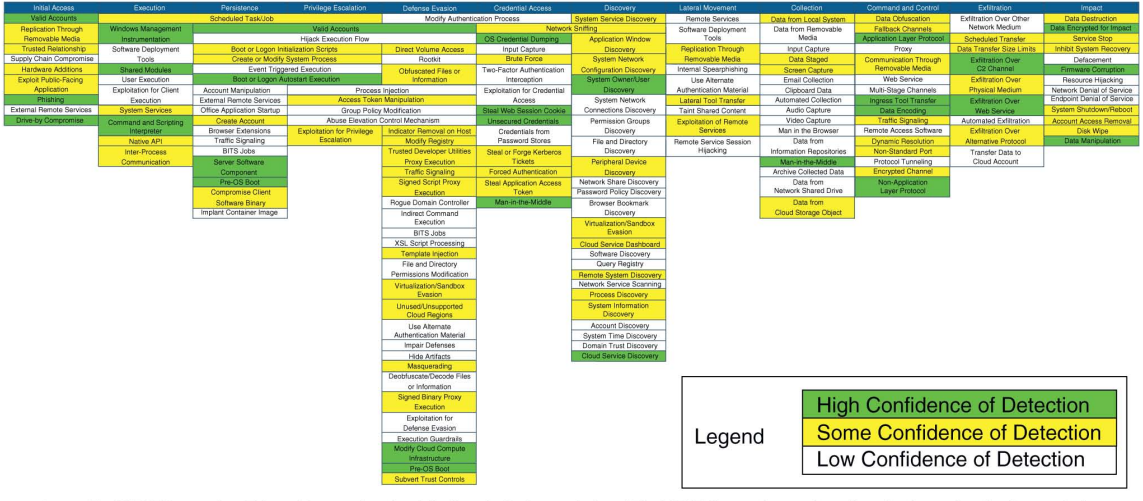
Organization	Name referring to vulnerability
AXENT (now Symantec)	phf CGI allows remote command execution
BindView	#107—cgi-phf
Bugtraq	PHF Attacks—fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP—cgi-phf
CyberSafe	Network: HTTP 'phf' attack
DARPA	0×00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http—cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
SecurityFocus	#629—phf Remote Command Execution Vulnerability

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.16



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.17

Initial Access → Execution → Persistence → Escalation → Evasion → Access → Discovery → Movement → Data → Commands → Exfiltration



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.18