RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-R02F

A New, Radically Innovative US–CCU Cyber-Security Check List

Scott Borg

Director (CEO) & Chief Economist
U.S. Cyber Consequences Unit

John Bumgarner

Chief Technical Officer
U.S. Cyber Consequences Unit

#RSAC

Problems with Previous Check Lists

Conventional check lists of security measures, *including ours* . . .

- Make security sound like a static condition
- Focus attention inward, on the information systems, not outward, on what attackers might do
- Make it easy to lose sight of what each security measure is supposed to accomplish
- Deal with items one-by-one, but are only effective collectively
- Focus more on past problems than on future ones

Our 2007 US-CCU Check List Wasn’t *Bad*

Virtues

- Started from scratch, rather than based on previous check lists
- Based almost entirely on real experience in the field
- Included many guidelines that were *not* just focused on preventing penetration
- Written in simple, non-technical language
- Made available for free

Signs It Was Useful

- Put into extensive use within weeks of its release
- Translated into many languages
- Used in over 80 countries
- Still being referenced and studied
- Probably the most widely used check list that isn’t an official standard

But we wanted to tackle the deeper problems

How do we make a check list that is . . .

- More dynamic in outlook?
- Focused more on the attackers & what they might do?
- Constantly drawing attention to what each security measure is supposed to accomplish?
- Holistic and systematic, rather than just a list?
- Oriented toward future security problems?

First, by Starting with the Attackers

The Five Steps in Any Successful Cyber Attack
(i.e., five hurdles an attacker must overcome)

1) Find the Target

2) Penetrate the Target

3) Co-opt the Target

4) Conceal What Is Being Done

5) Make It Irreversible

Second, by Looking at *All* the Attack Avenues

The Six Types of Components in an Information System

1) Hardware

2) Software

3) Networks

4) Automation

5) Human Users

6) Suppliers

(each with further sub-systems)

Third, by Combining These into . . .

The Basic US-CCU Cyber-Security Matrix

	Findable	Penetrable	Co-optable	Concealable	Irreversible
I. Hardware Components					
II. Software Components		All the Potential Attack Techniques & All the Technical Counter-Measures			
III. Network Components					
IV. Automation Components					
V. Human Components					
VI. Supplier Components					

This matrix can be read . . .

Vertically, to provide an attacker's viewpoint

Horizontally, to provide a defender's viewpoint

The Basic US-CCU Cyber-Security Matrix

	Findable	Penetrable	Co-optable	Concealable	Irreversible
I. Hardware Components					
II. Software Components					
III. Network Components					
IV. Automation Components					
V. Human Components					
VI. Supplier Components					

If populated with *offensive* tools and techniques . . .

These are well-distributed across all the boxes

The Basic US-CCU Cyber-Security Matrix

	Findable	Penetrable	Co-optable	Concealable	Irreversible
I. Hardware Components	●	●	●	●	●
II. Software Components	●	●	●	●	●
III. Network Components	●	●	●	●	●
IV. Automation Components	●	●	●	●	●
V. Human Components	●	●	●	●	●
VI. Supplier Components	●	●	●	●	●

If populated with *defensive* tools and techniques . . .

These are mostly concentrated in two boxes, with a few useful tools in two others

The Basic US-CCU Cyber-Security Matrix

	Findable	Penetrable	Co-optable	Concealable	Irreversible
I. Hardware Components					
II. Software Components		⬤			•
III. Network Components		⬤		•	
IV. Automation Components					
V. Human Components					
VI. Supplier Components					

To make the US-CCU Matrix more effective, we . . .

- Changed the labels to emphasize defense
- Added a column to cover “Overview” activities
- Filled in much more of the matrix than current standard practice
- By doing so, made it easier to see where new measures are needed

THE US-CCU CYBER-SECURITY MATRIX

	Overview	Harder to Find	Harder to Penetrate	Harder to Co-Opt	Harder to Conceal	More Reversible
I. Hardware						
II. Software						
III. Networks						
IV. Automation						
V. Users						
VI. Suppliers						

The new matrix labels and organization . . .

- Make cyber security outward looking, focused on the specific attack activities each defensive measure is supposed to stop
- Present each measure as a way of *actively* defeating an attack action, rather than achieving or maintaining a static condition
- Remind users to think of attackers as resourceful and creative
- Make it easier to focus on increasing attacker costs

You can't stop an attacker with enough resources, but you can increase their costs beyond what they would be willing to pay!

1) Making the Targets Harder to Find

- Force the attacker to spend much more time searching, researching, and mapping
- Make the attacker’s research obsolete sooner and more often
- Cause the attacker to waste time and resources on dummy targets that don’t yield anything
- Make the attacker worry about uncovering bogus information that will useless or even harmful to anyone trying to use it

2) Making the Targets Harder to Penetrate

(Doing what cyber security has already been doing)

3) Making the Targets Harder to Co-opt

- Make it harder for the attacker to understand how internal operations are carried out
- Make it necessary for the attacker to go through more steps to co-opt the system
- Reduce the ways in which the system can be readily manipulated
- Make the system continually self-correcting or self-restoring

4) Making the Attack Harder to Conceal

- Look for more symptoms, types, and correlates of attacker activity
- Lure the attackers into doing more things that will betray their presence
- Force the attacker to go to carry out more steps to conceal what is being done
- Make our detection efforts harder to subvert

5) Making the Effects More Reversible

- Capture and preserve more of the information and conditions that would be disrupted as a result of an attack
- Improve the systems and activities that substitute for the normal ones as a result of an attack
- Find ways to undo more of the effects of the attack
- Reduce the gains to the attacker by finding ways to take away the benefits the attacker has achieved (e.g., poisoning things the attacker might steal)

Using the New Matrix to Analyze Attacker Options

- A map for identifying the paths and successive actions an attacker would need to carry out
- A guide for estimating the time and skill levels needed for a given attack (i.e., attacker costs)
- A tool for analyzing and classifying multi-function malware
- A method for determining how attacker costs can be most cost-effectively increased

No defensive measure has failed if it substantially increases attacker costs!

Using the New Matrix to Evaluate Defenses

- A method for assessing the collective effectiveness of accumulated defensive measures
- A way of comparing and evaluating defensive products and services
- A basis for quantifying Vulnerability in a way that can be utilized in a rigorous risk analysis

What You Should Do Right Away

- Check off your organization’s answers! Ask yourself the reason for each unchecked item! (Avoid the excuses for dodging the question!)
- Treat the “checkmark boxes” as a *starting point, not a goal*!
- Consider implementing any unchecked items that would greatly increase *attacker costs* at a modest cost to your organization!
- Stop thinking of your job as maintaining confidentiality, integrity, and availability!
- Start thinking of your job as foiling attacks by making it prohibitively expensive for attackers to successfully carry them out!

How to Continue This Effort

- Suggest additional items for this matrix! Despite its length and the long research effort, this is *only a draft*!
- Help us expand the range of measures and tools, not for stopping penetration, but for economically defeating attackers!
- Look for a final, numbered version of the US-CCU Matrix later this year (and in other languages, assuming there is enough sponsorship)
- The US-CCU Matrix is easy to read and available for free! Share it with anyone you know who might be interested!

www.usccu.us

What We’ve Tried to Cover in This Session

- What to expect from the new US-CCU Cyber-Security Matrix
- The thinking behind the US-CCU Matrix
- Some of the ways to use the US-CCU Matrix
- How and where to get started
- Our plan for further revising and disseminating the US-CCU Matrix

Please send any suggestions for the US-CCU Cyber-Security Matrix to: checklist@usccu.us
(We will mention you by name in the introduction if you are the first make a suggestion we can use.)

To obtain other information, inquire about associated courses, offer sponsorship, or volunteer translation help, please contact:
scott.borg@usccu.us
and/or john.bumgarner@usccu.us