
# The 3Cs: Enemies of Cybersecurity

Whitepaper

Crytica Security
7655 Town Square Way, Suite 212
Reno, NV 89523

Website: CryticaSecurity.com
Email: info@cryticasecurity.com

# The 3Cs: Enemies of Cybersecurity

## Contents

# 1. INTRODUCTION

Amid a growing pandemic of cyber-attacks, both state-sponsored and criminal, Cybersecurity has become essential to the cyber world. As such, cybersecurity has become one of the most rapidly growing branches of the much broader field of security. Despite its "cyber" component, cybersecurity shares significant attributes with its parent discipline, as well as with the other branches of security. Among these attributes is the basic principle that: Security is far more a function of psychology and sociology than it is of technology. It is far easier to penetrate defenses by using social engineering than it is using weaponry and brute force; far easier to persuade someone to open a vault door than explode the vault open.

Recognizing that this human component is inherent to all security, it is clear that, foundational to all effective security is the principle that all individuals involved must:

- Be aware of the dangers
- Maintain the appropriate level of vigilance
- Know what to do in case of an attack.

## The 3Cs

An inescapable corollary to security's human-component principle identifies three very powerful forces that are antithetical to all security. These are known as the 3Cs (three "C"s). They are:

- Complexity
- Confusion
- Complacency

Unfortunately, in most widely adopted cybersecurity canons, in most widely used cybersecurity technologies, and in most widely adopted commercial cybersecurity offerings, the 3Cs are ubiquitous. This is one of the primary reasons why, by all objective measures, the cybercriminals are winning.[1]

Only by minimizing the 3Cs (they can never be completely eliminated) can cybersecurity systems become fully effective and functionally viable. This minimization is accomplished through understanding the 3Cs, that is:

- Knowing what they are.
- Being aware of what causes them.

[1] Numerous articles support the view that the cybercriminals are winning. Links to two recent ones:
https://www.thecipherbrief.com/why-cyber-criminals-are-winning
https://business.gmu.edu/news/2022-02/cybercriminals-are-winning-why-dont-consumers-care

- Being able to identify them when they exist.
- Having the strength, convictions, and abilities to combat them.

Until cybersecurity's 3Cs can be minimized, the cybercriminals cannot be effectively repulsed, and the cyber world cannot be fully imbued with some minimum modicum of functional security. The purpose of this whitepaper is to raise an awareness of, and create a level of vigilance against, the 3Cs. To do so, it examines each of them in turn and provides the beginnings of the requisite level of understanding.

## 2. COMPLEXITY

Complexity comes naturally to all human-designed systems. It is the unwanted but inevitable stepchild of large organizations and bureaucracies. It is the default design choice whenever insight, creativity, foresight, and artistic talent are lacking. It is also the design choice that leads, inevitably, to ultimate failure. Complexity tends to engender more complexity, which in turn engenders even more complexity, until the entire edifice collapses under its own weight.

### Some of the Deleterious Effects of Complexity

When a system is complex, it is inherently insecure.[2] For example, when a system is complex, it is easy for users to:

- Forget and/or overlook specific required steps.
- Confuse the proper order of required steps.
- Consciously avoid performing certain essential but onerous steps and take "short cuts". People, by nature, look to minimize their workload. If circumventing certain security requirements can make life easier for them, many people will choose circumvention. For example, if entry into a building through the appropriate entrances requires a complex rigamarole of procedures, it is common for residents to leave a backdoor or window unlocked/propped-open. They do so in order to simplify the process of entering/returning.
- Not comprehend the "big picture", the "why and how" of what the goal of the system is. Without comprehension, users perform tasks by rote and not with understanding. The result is a level of robotic stupidity that is unable to adapt to even the most minor, yet inevitable, unexpected situations.

When a system/process is too complex, its adoption and use engender resistance. This type of resistance is closely related to the well-documented phenomenon of "Resistance to Change". Its recognized symptoms include, in order of both chronology and severity:

[2] "Complexity can be the enemy of security. According to the findings, complexity can prevent companies from preventing data breaches.", *The Cybersecurity Illusion: The Emperor Has No Cloths,* Ponomon Institute Research Report, July 2019, p. 10.

- Denial ("we really don't have to do this")
- Ridicule and snide remarks ("What a dumb system! Whose idea was this?")
- Avoidance and failure to comply with the requirements
- Sabotage

## Why Is Complexity So Common?

If complexity is so fraught with problems, why is complexity so common, especially in cybersecurity systems? In science, there exists the principle of Occam's Razor. That can be paraphrased as: the simplest explanation is the best explanation. If science strives to adhere to Occam's Razor, why is this principle not an integral part of cybersecurity?

### *Simple Is Hard*

Simply put: "simple is hard." Complexity insinuates itself into system design in many ways. For example:

- When a "simple" solution is not immediately obvious and/or time pressure forces designers to adopt the "quick-and-dirty" approach, the result is often a design that is overly complex; one that then tends to be perpetuated through the phenomenon known as "design inertia."
- When the overall total picture is not seen and/or not considered, sub-optimal, complex partial solutions are adopted.
- When a simple functioning system is patched with a quilt of sub-optimal and complex patchwork of "fixes" the result is almost always a design that is overly complex.
- When simple designs elude the designers (a very common occurrence), complex designs are adopted, and these designs are rarely revisited.

It is a painful lesson of engineering that it is often much "easier", at least initially, to "design complex" than it is to "design simple." When someone does not know how to solve a problem, complexity is invoked to provide the appearance of a solution, even though a real solution has eluded them. It is the old principle of: "If you can't dazzle them with brilliance, baffle them with BS!"

### *Simple is Harder to Sell*

Another, perhaps less obvious, reason is that, in general, "simple" is harder to sell than complex. Many people will pay more for what they don't understand. There is a mistaken perception that complexity equates to sophistication. The reality is that the exact opposite is true.

### *Security Through Obscurity*

A classic example of the appeal of complexity is the widespread use of "Security Through Obscurity". Security through obscurity can appear to its proponents and practitioners to be very effective. The use of complexity/obscurity certainly provides

an aura of sophistication. It can create a grand illusion of security. Unfortunately, it is only an illusion. Three of the most common versions of Security Through Obscurity are:

- Security through "complexity": The theory is simple. Make the security so complex and so confusing that the enemy will not be able to figure it out. Ultimately, they will get frustrated and give up. History has shown, time and again, that the reality is quite different. Typically, the complexity confuses those whose job it is to implement the security; confuses them to the extent that mistakes are made, and thereby the security is compromised. At the same time, a determined enemy (if the prize is big enough) will make the required effort and take the required time to work through all the complex security's labyrinthine details. The result is that ultimately the security is compromised.

  Note: Some may ask the question that: If cybercriminals can analyze complex systems, will not simple systems be that much easier for them to analyze? The answer is, of course, "yes". However, the simple systems to not rely upon the element of complexity for their security. They employ other measures in order to deter the cybercriminals, simple to understand, deploy, and employ, but not simple to overcome.

- Security through "secrecy": The theory is that if only a privileged, trusted few know the secret of the security, the security will be effective. While the secret is kept, the security will be maintained. One problem with this approach is that the moment more than one person knows a secret, it is no longer a secret. Another is that, once the secret, the keystone/linchpin, is no longer a secret, the entire security edifice can collapse rapidly and catastrophically.

- Security through "magic": Magic is perhaps the most insidious type of obscurity. It involves the use of a "trusted" but not fully understood component as the basis for the security. The argument goes: "If we have the secure '*xyz*' component in our system, our system is secure because the component is intrinsically and unquestionably secure." In this scenario, the possibility is ignored that the trusted component is somehow vulnerable. In this blind faith, some of the most basic security tenets are disregarded. These tenants say:

  a. A system is only as secure as its weakest link.

  b. There is no such thing as 100% security; any and every "wall" can and will be penetrated.[3]

  Very much akin to the concept of *Deus ex machina*, security magic removes the evaluative analysis of security from the realm of logic/reason and places it squarely into the realm of faith.

The result in all these cases is compromised security.

[3] Attributed to George S. Patton: "Fixed fortifications are monuments to the stupidity of man."

## 3. CONFUSION

Confusion is the relative of ignorance. When a person is ignorant, that person, due to a lack of information, does not know what to do. When a person is confused, that person, due to a lack of comprehension, does not know what to do. The dangers of confusion are well known. In the face of a dangerous threat, confusion can lead only to missteps and errors. These errors can often be catastrophic.

### Some of the Causes of Confusion

Discussed above is the concept that complexity can cause confusion. Other causes include:

- Lack of clear understanding.
- Lack of clear and/or complete instructions.

#### *Lack of Clear Understanding*

Environments requiring security are dynamic environments. They experience a vast and ever-changing array of conditions and challenges. Not all conditions and challenges can be anticipated. To respond intelligently to the unanticipated and to the unexpected requires a level of reasoning and analysis that is only possible when it is based upon a clear understanding of the functions of the environment and the types of threats to which that environment may be subject. Where there is no clear understanding, challenges engender confusion, confusion engenders errors, and errors engender catastrophes.

#### *Lack of Clear and/or Complete Instructions*

There is an unfortunate trend in many enterprises today. This trend is to infantilize and de-humanize staff. Staff are told: Do not think! Just follow the instructions! This "staff-as-robot" policy is unfortunate for many reasons. From strictly a security standpoint the shortcomings include:

- Incomplete Instructions – not all eventualities can be anticipated. Thus, when an unanticipated situation arises, staff are clueless as to what to do; and being unaccustomed to thinking for themselves and making critical decisions, the probabilities are that the decisions made will be the wrong ones.
- Unclear Instructions – when instructions are unclear, robotic staff are forced to think for themselves and make decisions in an environment that discourages independent thinking. Once again, the probabilities are that the decisions so made will be the wrong ones.

Whatever its cause(s), confusion is the bane of effective security.

## 4. COMPLACENCY

Effective security must be based upon an awareness of the threats and the constant vigilance required to detect those threats as quickly as possible. One cannot be vigilant if one is not aware of the possibilities of, and potential for, danger. When one

is complacent, one is neither aware nor vigilant. A complacent target is the perfect target for an attacker, since it neither expects an attack nor is on the lookout for one. Indeed, many famous military campaigns have been won through the presence of complacency in the enemy.[4] This is as true of the cybersecurity realm as it is for the other security realms.

Those on the frontlines of cybersecurity, those laboring "in the trenches", know all too well the dangers of complacency and how insidiously widespread it is. As one frontline professional has stated:

> Complacency is by far the most dangerous of the obstacles to the propagation of effective security measures. Experience teaches us that complacency takes many forms, posturing in many different positions. These include such common mindsets as: "we are adequately protected", "we already have that", "we already have a fully deployed solution", and "our managed services provider has that covered for us." These mindsets enable decision makers to ignore all the reputable cybersecurity statistics, as well as the well-documented rampaging wildfire of ransomware; even though both these data sets are strong proof that the oft-repeated highly confident mantras noted above are tragically self-deluding. There can be no doubt that the proponents of these complacently confident beliefs are grossly mistaken. And yet, even in the face of all the evidence to the contrary, until it happens to them, these same proponents remain depressingly unshaken.

## 5. SOURCES OF THE 3CS IN CYBERSECURITY

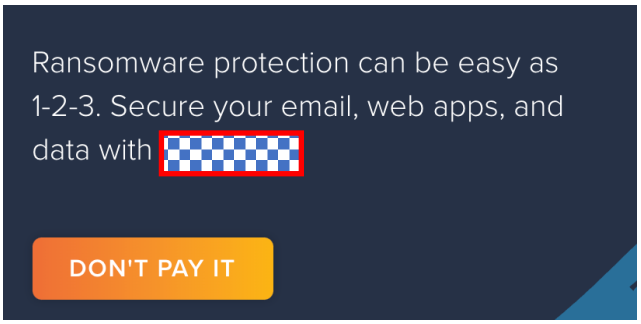
When looking at the sources of the 3Cs in Cybersecurity, it is logical to consider them in reverse order, i.e., Complacency, Complexity, Confusion.

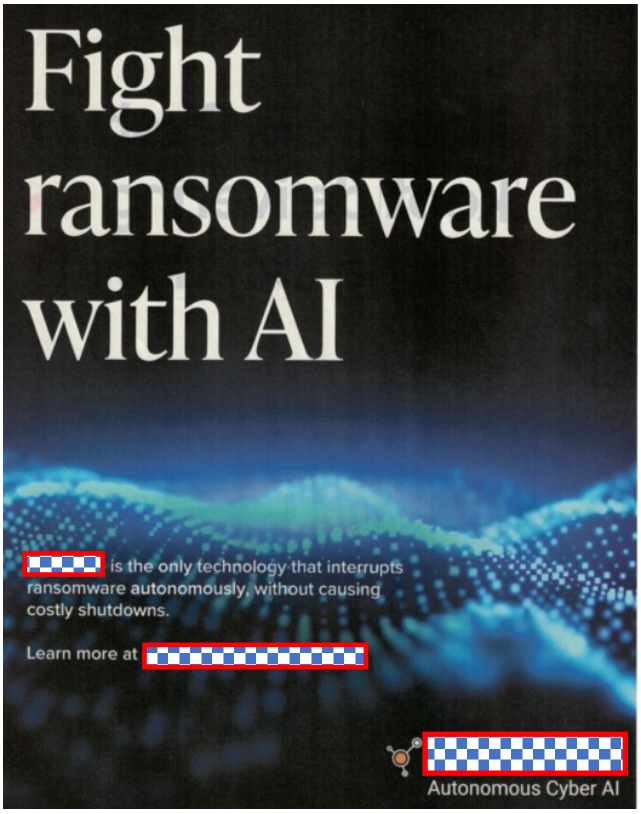
### Complacency

A cursory scan of the marketing hype that is so pervasive in the Cybersecurity industry reveals some of the primary culprits in the ubiquitous complacency that casts such a broad dark shadow across almost all sectors of the cyber world. Consider:

[4] Some examples include: how the Mongols breached the Great Wall of China (1213-1214), why the Germans were so successful in the early stages of the Battle of the Bulge (1944-1945), and why the Egyptians were so successful against the Israelis in the early stages of their 1973 war.

- Ads such as those that claim:




- Initiatives and technologies that use terms implying untenable levels of "trust", terms such as "Zero Trust" and "Trusted Computing".

Why are these examples so detrimental? Because they create a false sense of security, and thereby induce dangerous levels of complacency. Consider, for example, the false claims as to how effective some cyber defenses are. If a cybersecurity vendor claims:

- "Ransomware protection can be as easy as 1-2-3" - That claim tends to instill an unrealistic level of confidence in that vendor's customers. This level of confidence is especially unrealistic when ransomware attacks are running rampant and the average Dwell Time (the time between malware infection and malware detection) for the best protected systems is longer than 180 days.[5]

[5] IBM Corporation. (2021). (publication). Cost of a Data Breach 2021. Armonk, New York.

The net result of a such a claim is to create a false sense of security in the face of clear and present danger.

- "Fight ransomware with AI [Artificial Intelligence]" - That claim conveys the message that ransomware can be consistently detected and defeated using the mystical/magical tools of AI. For most people, AI's ransomware detection/defeating technology is so esoteric that it falls into category of magic, per Arthur C. Clark's Third Law: "Any sufficiently advanced technology is indistinguishable from magic."[6] However, one does not need to understand the intimate details of AI to realize that AI alone is not a sufficient, nor even a very wise, defense against ransomware.

  AI is merely a tool, albeit a very sophisticated one. As with all tools, it can cut both ways. The AI used to protect against ransomware can be used with equal, and perhaps even greater efficacy by the cyber criminals to defeat a defender's AI.[7] The result is a perpetual AI arms race, one that, by using AI alone, the defenders can never win. AI, while being a very powerful tool, cannot, by itself, provide the level of protection implied by the advertising. By invoking the magic of AI, vendors create the impression of a level of power, competency, and security that the technology cannot support. The net result of a such claims is to create a false sense of security.

- The rampant use of misleading terminology and technobabble – This practice is also highly counter-productive. Consider, for example, terms such as "Zero Trust" and "Trusted Computing" et al. In the world of security, the term "trust" must always be regarded with suspicion and is never to be trusted. President Ronald Reagan popularized the English phrase: "Trust but Verify"[8]. In security, especially in cybersecurity, the necessary order is reversed: Verify first and then trust … but even then, trust only partially. One must always continue to reevaluate and re-verify. "Trust" and "security" are mutually exclusive.

  One very prominent example of misleading terminology is the highly touted cybersecurity approach: "Zero-Trust". In practice, Zero-Trust does not employ "zero trust". Under its principles, users are vetted first before being granted access to resources, before being "trusted". Thus, at best, the term "Zero-Trust" is both highly ambiguous and highly misleading. "Zero" trust in a cyber system is a meaningless phrase. Systems cannot operate merely on their own. "Some person", and usually many people, must be trusted for a system to operate. The more people who must be "trusted", the more vulnerable the

[6] Clark, Arthur C., "Hazards of Prophecy: The Failure of Imagination" in the collection Profiles of the Future: An Enquiry into the Limits of the Possible (1962, rev. 1973), pp. 14, 21, 36

[7] It has already been noted by some authors that the cybercriminals are winning the cybersecurity AI arms race. For example: https://www.globenewswire.com/en/news-release/2022/05/03/2434678/0/en/Research-Shows-Security-Pros-Believe-Cybercriminals-are-Winning-the-AI-Race.html

[8] This is a direct translation of the original Russian proverb: Доверяй, но проверяй.

system is. Unfortunately, the phrase "Zero-Trust" conveys both an impression of a highly untenable level of security, and a logical contradiction (truly zero trust is impossible). This leads to both complacency and confusion.

There is also a component of the magical in all "trust" technologies. When users trust, they tend to no longer verify, no longer question, no longer apply reason and understanding, and no longer remain vigilant. Where there is no vigilance, there is no security.

The marketing claims and the overly hyped terminology create detrimental levels of confidence and destructive levels of a false sense of security. They create an atmosphere of complacency in an environment and at a time when maximum vigilance to required.

## Complexity

Some of the reasons for, and the deleterious results of, complexity are explored above.

## Confusion

Confusion comes in many different guises. Consider just a few examples. There is the confusion that results from:

- The vast and variegated array of cybersecurity products and services.
- The conscious obfuscation by the various cybersecurity vendors, an obfuscation implemented intentionally to impart a greater aura of efficacy and sophistication to their products/services.
- The complexity inherent in the designs of many of the arcane and esoteric cybersecurity technologies.
- The complexity inherent in many currently implemented cybersecurity policies and procedures.
- A cyber-attack for which no policies and procedures exist.
- A cyber-attack that successfully by-passes and/or disables all the existing cyber-defenses; leaving defenders to improvise and fend for themselves.

There can be little doubt that confusion is not a desired state in almost any environment. In the cyber world, it can be catastrophic. And yet, in the cybersecurity realm, confusion seems almost inevitable. Consider:

- When headlines blare a barrage of breach stories and vendors hawk a panoply of unrealistically effective cybersecurity tools, confusion is inevitable.
- When the mainstream cybersecurity tools become ever more arcane and when these tools rely ever more heavily on magic, confusion is inevitable.
- When the cybersecurity tools are becoming ever more complex, and end-users are instructed not to think and not to reason, confusion is inevitable.

- When so much of the cybersecurity world is being baffled by B.S. rather than being dazzled by brilliance, confusion is inevitable.

## 6. MINIMIZING THE 3CS

### Confusion

An antidote to confusion consists in recognizing Occam's Razor, that the simplest solutions are the most effective. It consists in designing cybersecurity defenses in such a manner that they do not rely upon complexity and obscurity as the basis for their security. It consists in deploying cybersecurity systems that do not rely upon "magic" and do not rely upon an implicit endless technological arms-race to stay ahead of the cyber criminals. Consumers must demand comprehension and understanding of the principles of the systems they acquire.

Another antidote to confusion consists in staff education. Education goes beyond mere "training". "Education" includes comprehension and understanding, not merely instructions to be carried out by rote. Staff and all involved must be educated about the functioning of the systems and the real dangers that threaten it. When confronted with the unexpected and unanticipated, it is only through understanding that intelligent decisions can be made.

### Complexity

Some of the antidotes to complexity are:

- Requirements for simplicity to always be a high priority design criterion, for all elements of the overall architecture and implementation.
- Requirements for complete comprehensibility of the principles of all aspects of an entire system. By requiring comprehension, and the necessary propagation of that comprehension, the need to keep concepts simple will be forced upon the propagators.
- Recognition that all systems are "living" evolving entities. Change, for them, is inevitable. As such, all systems must be designed to evolve and change. Complexity renders change and evolution much more difficult. Simplicity makes evolution possible.

### Complacency

Awareness and vigilance are necessary components for all security. Despite a cultural tendency toward denial, toward seeing the world as being essentially benign, the world, especially the cyber world, is a very dangerous place. It is not a cartoon world in which one can walk off a cliff but not begin to fall until one looks down and realizes that one is walking on air. In the cyber world, we need to be constantly looking down … and looking up … and looking in all directions. The threats are coming at us from all directions. Only education, and re-education, reminding and re-reminding can overcome our natural desires to feel secure and our cultural inclinations toward denial.

## 7. AN EXAMPLE OF A NON-3CS CYBERSECURITY SYSTEM

An example of a cybersecurity system that does not fall prey to the 3Cs is Crytica Rapid Detection & Alert (RDA) system, with Persistent Detection™. It was created to solve one problem and only one problem: How to reduce average malware Dwell Time from many months to mere minutes. The premise is a very simple one: If you cannot detect malware in a timely and actionable manner, you cannot protect.

The solution is also easy to comprehend.

- Crytica's system does not rely upon vast databases of virus signatures, complex to create and complex to maintain.
- Crytica's system does not rely upon historical data of any kind, not even the historical patterns of system/human behavior.
- Crytica does not rely upon AI-based and probabilistic predictions. Its algorithms are deterministic, not probabilistic. Therefore, it is not subject to the myriad false positives that plague the AI-based systems.
- Crytica **does** rely upon the principle that: Any unauthorized change to how a computer operates, i.e., any unauthorized changed to a computer's instruction set, is, by definition, malware.

Hence, the Crytica detection engine is designed to detect all unauthorized changes to how a computer operates. This principle is not complex and not difficult to understand, even though the actual engineering and programming behind it is non-trivial.

## 8. NEXT STEPS

To find out more about how to eliminate some of the 3Cs by using Crytica's Rapid Detection & Alert (RDA) system with Persistent Detection™, and to understand more about Crytica's no BS, no nonsense, no confusion, and minimum complexity approach to cybersecurity, contact Crytica Security, Inc.

**Website:** CryticaSecurity.com
**Email:** info@cryticasecurity.com