How to Think Like a Cybersecurity Defender

Doc Blackburn

Vera's Origin Story

Vera has been given an opportunity at work.

She was promoted from the IT Help Desk to a **Junior Security Analyst**.

Walking home she sees her neighbor, **Walter**.

Let me introduce you to someone, Vera.
Vera just landed her first job working in cybersecurity. She's excited. She's motivated. And like a lot of people entering this field for the first time, she wants to do well.
So she starts doing what most of us would do. She buys books.
Networking books. Incident response books. Cryptography books. Cybersecurity books.
Every night she goes home, opens those books, and studies. She highlights things. She takes notes. She memorizes terminology.
But something strange starts to happen.
The more she reads... the more confused she becomes.
Every book talks about different tools. Different technologies. Different frameworks. Different ways of doing things.
And she starts to wonder if she's missing something.
One evening she's walking home carrying yet another stack of books when someone notices her.

Learning Security?

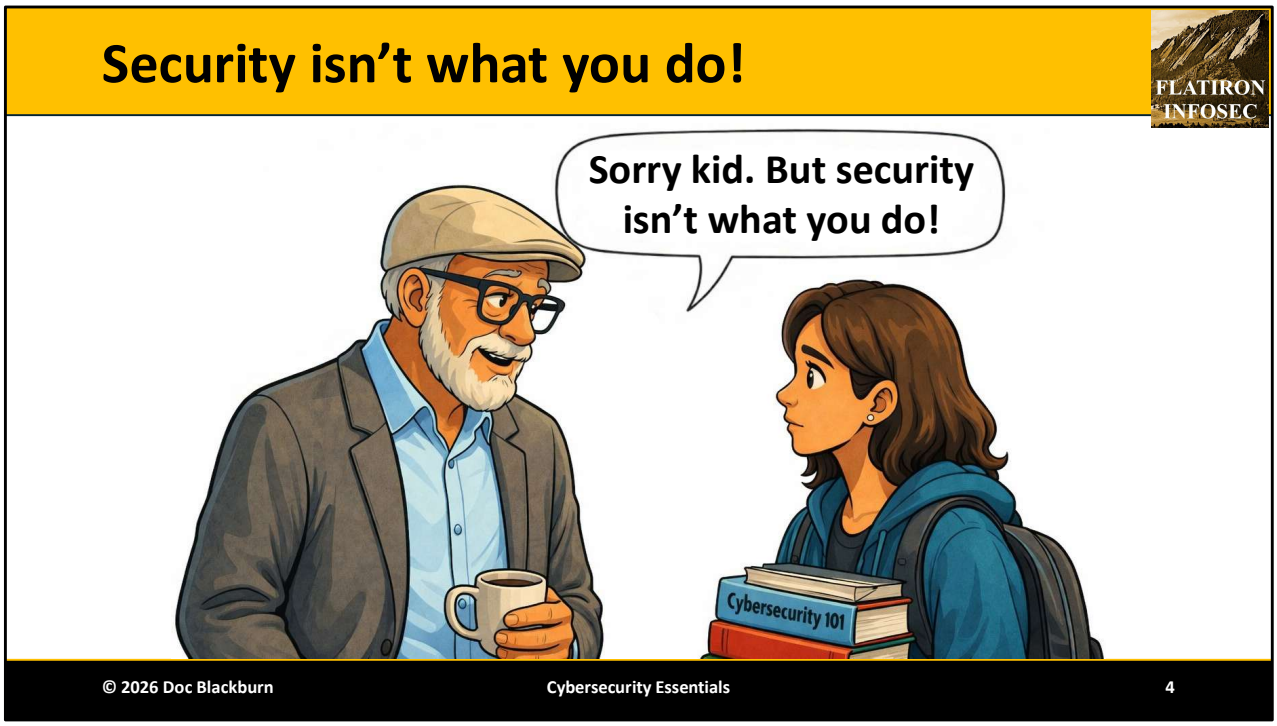
Vera: I got a promotion at work. I'm going to be a Cybersecurity Analyst!

Walter: Cybersecurity, huh? Did you know that's what I did? Started in the Army. Retired as a CISO.

Vera: I didn't know that! What can you tell me about it?

Walter: Well, I know that the answers you're looking for are not in those books.

That someone is Walter.
Walter is an old family friend. Vera has known him since as long as she could remember. He lives a few houses down, and on most evenings, you can find him sitting on his porch with a cup of coffee.
Walter sees Vera walking down the street carrying this huge stack of cybersecurity books.
He smiles.
Vera stops and says hello. They exchange a few words like neighbors often do.
Walter looks at the books and says something simple.
"That's a lot of studying."
Vera nods and tells him she just started working in cybersecurity and she's trying to learn everything she can.
Walter listens.
He doesn't interrupt. He doesn't lecture.
He just listens.
And when she finishes explaining everything she's been reading and studying... Walter leans forward just a little bit and says something that completely stops her in her tracks.



Walter looks at her and says:
"Sorry kid... but security isn't what you do."
Now imagine how confusing that must sound.
Vera is thinking:
What do you mean security isn't what you do?
Isn't that exactly what I was hired to do?
Walter smiles because he can see the confusion on her face.
And then he explains something that takes many people years to realize.
"Cybersecurity isn't really about tools. It's not about memorizing products. And it's not about learning one specific technology.
Cybersecurity is about learning **how defenders think**. It's about understanding risk. It's about understanding how systems fail.
And it's about understanding how attackers look at the world."
That's what this workshop is really about.
We're not going to focus on memorizing tools.
Instead, we're going to focus on the **mental models defenders use to understand and protect systems**; concepts like least privilege, the CIA triad, and the balance between prevention, detection, and response.
Because once you understand how defenders think, everything else in cybersecurity starts to make more sense.

Vera looks at Walter, confused.
“Security isn’t what you do?”
Walter chuckles a little and takes a sip of his coffee.
Then he says something that changes the way she thinks about the field.
“Security isn’t a task.
It’s not a tool.
And it’s definitely not a product.”
He points to the stack of books in her arms.
“All of those books are trying to teach you *what* to do.”
He pauses.
“But real security professionals spend most of their time figuring out **why things fail**.”
Vera is still listening carefully now.
Walter continues.
“Every system has weaknesses.
Every design has trade-offs.
And every defense eventually gets tested.”
Then he gives her the real lesson.
“Security isn’t about making systems perfect.
It’s about understanding **risk**, **failure**, and **trade-offs**.”
Walter leans back in his chair.

“Once you understand that… all the rest of the stuff starts to make sense.”

Introduction to Cybersecurity

Absolute Truths of Cybersecurity

Principal of Least Privilege

Confidentiality, Integrity, and Availability (CIA Triad)

Prevention, Detection, Response

Absolute Truths of Cybersecurity

Introduced by

Keith Palmgren

Over a long and storied career Keith had found that there are specific, inescapable, and immutable facts about cybersecurity. He has graciously allowed us to use his

14 Truths of Cybersecurity

I will argue with him.
But the truths still hold.

Truth #1

There is no such thing as security, only varying degrees of insecurity.

Zero Risk Does Not Exist

Security ≠ Binary

Degrees of Insecurity

Perfect Security = Myth

One of the most important facts we must not only acknowledge but internalize and make a part of our collective consciousness is that there is no such thing as zero risk. Everything has risk. As people living life, we all understand this. But we don't think about it in our everyday life. We take that mindset to our work as well. It is easy to allow risk factors to slip out of our thoughts because we don't face constant threats.

Cybersecurity Through the Lens of Insecurity

The idea that "there is no such thing as security, only varying degrees of insecurity" encapsulates the reality that cybersecurity is not a binary state but a constant negotiation of risk. Every system has vulnerabilities, every control has limits, and every organization is exposed, just to different extents. Perfect security is a myth; what we actually manage are tradeoffs in exposure and impact.

This perspective forces a mindset shift: our role isn't to eliminate threats but to reduce the blast radius when—not if—something goes wrong. Security becomes less about control and more about resilience. The goal is not absolute defense but faster detection, smarter containment, and graceful recovery.

By acknowledging that all systems are inherently insecure, we dismantle dangerous expectations of perfection and begin building realistic, sustainable security programs. It's a humbling view but also an empowering one. It lets us stop chasing the impossible and start defending what truly matters.

Truth #2

The network doesn't exist to be secured.

The Network Supports the Mission

Usability vs Control

Functionality vs. Security

This truth is related to and very similar to Truth number one. Yet it is a distinctly different way of looking at insecurities. No network, system, or application has been created simply to secure it. Our organization certainly wasn't established to make it secure. Our organizations and the IT assets that support them exist to fulfill the mission. This gives way to the third truth.

The statement **"The network doesn't exist to be secured"** is a critical reminder that business infrastructure isn't built with cybersecurity as the primary goal. Networks exist to move data, connect people, enable transactions, and drive productivity. Security is a necessary overlay, not the reason for the network's existence.

This truth has significant implications. When security teams approach infrastructure as something to be "locked down," they often clash with the reality that networks must be open enough to support collaboration, customer access, remote work, vendor integration, and more. The result is tension between usability and control, often resolved in favor of business needs, leaving security teams scrambling to contain risk after the fact.

Understanding that the network wasn't designed for security helps shift the security mindset. Instead of trying to retrofit airtight protection onto something

inherently porous, our focus should be on building **resilience into what already exists**—detecting compromise quickly, containing threats effectively, and recovering rapidly. It's not about securing the network as an object; it's about protecting the mission it supports.

Truth #3

When security gets in the way of the mission – Security is wrong, not the mission

The Mission is Never Wrong

Security ≠ Objective

Security as Barrier = Failure

The mission is literally why we have a job

 Cybersecurity Essentials 10

Since the organization exists to fulfill its mission, security risks getting in the way of that.

This is the most important one on the list.

One of the most damaging delusions in our field is the belief that security is the primary objective. It isn't. The mission is the primary objective. Whether that objective is teaching students, delivering healthcare, shipping products, or supporting national security. Security exists to protect and enable that mission, not to control it.

Too often, security becomes an obstacle. We enforce rigid password policies that lead users to write credentials on sticky notes. We block tools essential to productivity because we can't secure them fast enough. We slow down development cycles under the banner of "zero trust," forgetting that the business survives on speed, not stasis.

When security gets in the way of the mission, it's security that's wrong, not the mission.

This doesn't mean abandoning controls or accepting reckless risk. It means designing security that aligns with operational realities. It means listening. It means flexibility. If we're not enabling the business to move faster, safer, and

smarter, we're failing at our job—no matter how many policies we enforce. Security must be a partner, not a barrier. Otherwise, we become irrelevant—or worse, actively harmful to the organizations we claim to protect.

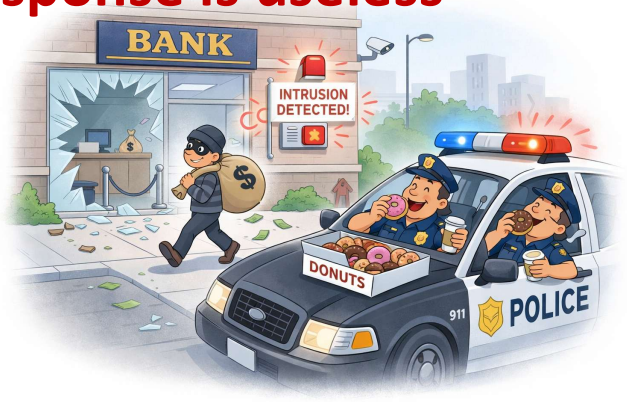
Truth #4

Prevention is ideal – Detection is a must.
Detection without response is useless

Prevention Will Fail

Detection Is Required

If You Cannot Detect
You Are Flying Blind



The saying **"Prevention is ideal – Detection is a must – Detection without response is useless"** captures the evolution of mature cybersecurity thinking. In an ideal world, every threat would be stopped before it starts—before the email is opened, the vulnerability is exploited, or the attacker gets a foothold. But we don't live in that world. Prevention fails. That's not a possibility—it's a certainty.

That's why **detection is non-negotiable**. If you can't detect when something goes wrong, you're flying blind. And yet, many organizations invest in prevention-heavy architectures with minimal visibility. They don't know when they've been breached. They don't know what's happening in their environments. Logs are missing. Alerts go ignored. Dwell times stretch into months.

But detection alone isn't enough. **Detection without response is a tree falling in the forest.** If your team doesn't act on alerts—if there's no playbook, containment strategy, or coordination— you're just collecting bad news faster. Too many breaches have been detected early but allowed to spiral out of control due to poor or delayed response. Equifax saw signs of compromise but failed to act. Target received FireEye alerts about their breach but ignored them.

SolarWinds attackers lived inside networks for months undetected—and when finally caught, responders were unprepared.
Prevention is the first layer. Detection is the safety net. But **the response is what actually stops the bleeding**. Without it, the rest is just noise. A mature cybersecurity program doesn't just try to prevent attacks; it prepares to survive them.

Truth #5

Security must always be driven by business need

Security Supports The Mission

Secure What Matters Most

Not Everything - Not Equally

Prioritize High-Impact Risk

Security must always be driven by business need. That's the anchor point of any effective cybersecurity strategy. If security operates in a vacuum—chasing threats, implementing tools, or enforcing controls without understanding what the business is trying to achieve—it becomes a cost center, a blocker, or worse, irrelevant. The purpose of security is not to secure everything equally—it's to secure what matters most to the business, in a way that enables the mission rather than interfering with it.

This is why **a solution without a problem is not a solution**. The cybersecurity industry is full of shiny tools that solve hypothetical problems, often pushed by vendors before organizations have defined their actual risks. Deploying a tool "just in case" or "because the Gartner quadrant says so" is not strategy—it's noise. Before implementing any control, we must be able to answer the following questions: *What specific problem are we solving? What business process does it protect? What would the impact be if we didn't solve it?*

This leads directly into a critical mindset: **"Before I spend a dollar of my money or an hour of my time, I need to ask: What is the risk? Is this the highest priority risk? And is this the most effective way to deal with it?"**

Security resources—budget, staff, time—are finite. Prioritization is essential. If

we spend resources on low-impact risks while critical exposures remain unresolved, we're not protecting the business—we're managing optics. Ultimately, aligning security with business needs means speaking the language of risk and value. It means understanding what the business cares about, what keeps stakeholders up at night, and what failure truly looks like. Security should never be about achieving a perfect control environment. It should be about helping the business move faster, safer, and with confidence—by managing the risks that matter most.
A solution without a problem is not a solution.
Security, while seen by its practitioners as a significant business function, has only one reason for existing. To protect the assets and processes of the organization so that the organization might reach its goals.

Unless the organization is a Security services firm, whatever the goals and vision of the leaders of the enterprise, that is what security is there for. We must realize that sometimes, the business is willing to take the risk associated with not having excellent or even good security tools and practices. While we may suggest advances in security capabilities and show how best to comply with regulators and other stakeholders, it is not security's role to decide how far that will be carried.

Therefore, security must understand and support the goals of the organization. We must know and understand the organization's most important initiatives to obtain support and funding for our security initiatives. Further, by showing how we support and prioritize the problems of the business, we become partners, rather than just a cost center they must pay for.

The Center for Internet Security maintains the Critical Security Controls list. This list, first created by SANS Institute, is "a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture." In order for a security control to be considered a high enough priority to be included on the list, it must meet the guiding principles. One of the guiding principles is that the defensive measure must be designed to address the most common cyber threats and vulnerabilities, aligning with the principle of mitigating high-impact risks.

Taking this a step further, in order to ensure that the control is adequately implemented, its impact must be measurable. If we cannot measure the value, we can't really say it has addressed the problem.

Truth #6

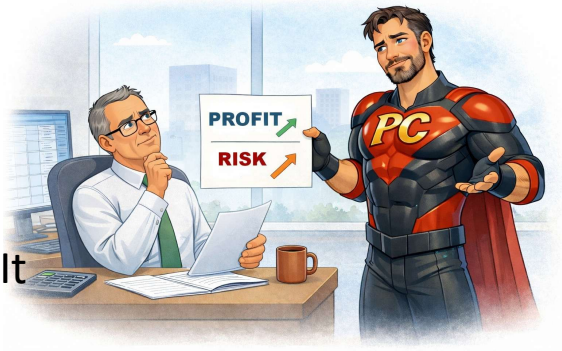
Security is a cost center, not a profit center

Security Protects Revenue

Reduces Loss

Optimize Security, Not Maximize It

Security Can Add Value By Minimizing Loss



It doesn't have to be this way. This statement is absolutely true, but we can reframe it. While it is true that security is not an activity that makes money as a core part of the business operation, security can help an organization meet its financial goals through savings and reducing losses. Security is the act of building repeatable processes that yield dependable results. That is also how to describe efficiency. Security and efficiency can be one and the same when mindfully crafted.

Security can provide timely warning signs. Security alerts can give us an early warning system of operational issues that may or may not be related to the actions of a threat actor. Security activities can include monitoring for loss of service (a breach of availability), a core tenet of security. In this sense, security is perfectly aligned with operational objectives.

Security is a cost center, not a profit center. That statement often makes security professionals uncomfortable, but it's a reality we must accept and work within. Security doesn't directly generate revenue. It doesn't close deals, ship products, or increase market share. Instead, it protects the ability to do those things without disruption or loss. That doesn't make security unimportant; it is a form of strategic insurance that protects the business's ability to operate and

grow.
Understanding security as a cost center helps frame decisions through a risk lens rather than a revenue one. Every dollar spent on cybersecurity must be justified by the value of what it protects or prevents. The goal is not to maximize security spending—it's to optimize it. That means identifying the most critical risks, selecting the most effective controls, and proving that the investment is proportionate to the threat. In a world of finite budgets, we can't protect everything equally and shouldn't try.
This also means security must compete for attention and resources alongside every other business function—sales, marketing, operations, and product development. To be taken seriously in that environment, we have to stop speaking in abstract technical terms and start speaking in the language of **risk, impact, and cost avoidance**. Boards don't fund firewalls—they fund reduced legal exposure, minimized downtime, and protection of customer trust.
When we stop pretending security pays for itself and start treating it as a strategic cost center, we can more effectively align with business goals, justify our role, and earn a seat at the decision-making table, not by selling fear, but by demonstrating measurable value in protecting what enables the business to succeed.

When security can find ways to better align itself with the objectives of the organization, it can help the organization fulfill its mission. In that sense, is it really just a cost center?

Truth #7

Security is a process… not a product

Tools Assist - Process Protects

Security Is How We Operate
People – Process – Technology

Security Isn’t Bought, It’s Practiced

This truth can be hard for the organization's stakeholders to understand. And we have not done ourselves any favors with the language we use to describe our security objectives, namely, compliance. We measure and quantify our cyber preparedness with security controls. As we discussed previously, controls imply that some sort of end state can be reached once the control is in place.

Security isn't something to be achieved. Security is how we operate. It is also not something that is added on. While there are some security practices we can put in place that are added on, the most effective and comprehensive security features are implemented into the design of the systems, processes, and the organization itself.

This simple distinction lies at the heart of many of the failures we see in modern cybersecurity programs. Products—firewalls, EDR, SIEMs, and identity platforms—are tools. They can help reduce risk, detect threats, and enforce policy. But on their own, they do nothing. Without skilled people, mature processes, and strategic alignment, a product is just shelfware—or worse, a false sense of security.

Many organizations fall into the trap of buying their way into security maturity. They chase the latest technology trends, assuming that the right tool will "solve"

security. But security isn't something you install—**it's something you practice**. It's an ongoing cycle of risk assessment, control implementation, monitoring, response, recovery, and improvement. Tools can assist in that cycle, but they don't replace it. In fact, the more tools you add without process maturity, the more complexity and alert fatigue you introduce.

A product cannot replace judgment. It doesn't know your business priorities, regulatory obligations, or operational realities. It can't build a security culture or foster accountability. That's the role of process—designed by humans, refined through experience, and driven by the mission. When we treat security as a process, we focus on outcomes instead of features, and resilience instead of checklists.

Ultimately, the organizations that succeed in cybersecurity are not those with the biggest toolsets, but those with the clearest processes for making informed decisions, responding to incidents, and adapting to change. Security isn't something you buy once. It's something you **do** daily, iteratively, and deliberately.

Truth #8

You cannot process encrypted data… EVER

Encryption Protects Stored & Moving Data

But Not Active Data

Processing Requires Plaintext

Decryption Creates Exposure

Attackers Do Not Break Encryption
They Wait For Decryption

That statement, while technically simple, carries profound implications for how we think about cybersecurity, privacy, and trust. Encryption is a mechanism for confidentiality. It protects data in transit and at rest by making it unreadable to unauthorized parties. But the moment you want to *do something* with that data—analyze it, display it, search it, transform it—you must first decrypt it. And once it's decrypted, it's vulnerable.

This truth is often glossed over in marketing for security tools that promise "end-to-end encryption" or "secure analytics." In reality, data must be in plaintext at the moment of processing, whether it's happening on a server, in memory, or on an endpoint. That moment—however brief—is a window of exposure. No matter how strong your encryption algorithms are, they cannot protect you during that moment when the data is actively in use.

The implication is this: **encryption is not a solution to all risk—it is a control with limits.** It buys you time. It protects you when data is at rest or in transit, but not during the critical point of interaction. This means attackers don't always need to break encryption—they just need to be present when and where the data is decrypted. This is why endpoint security, memory protections, and runtime controls are so important—and why trusting unverified environments

(like third-party cloud services or unmanaged devices) with sensitive data is inherently risky.
Recognizing this limitation forces us to design security with a more realistic mindset. If we can't protect data while it's being processed, we must focus on securing the environment where the processing is done. We must ensure that only the right users, systems, and processes ever reach that decrypted state—and that once they do, we monitor them closely. Trusting encryption blindly is dangerous. Respecting its limits is essential.

There is a crucial point to this truth. First, we need to unpack what encryption does for us. Encryption of our data is the best method of protecting our information when we are not accessing it. The premise is that if we have properly encrypted our data, when a threat actor has the opportunity to steal a copy of it, the encryption protects the data from being read by the threat actor.

We encrypt information for many different reasons. However, the most common reason is to protect against unauthorized disclosure, also known as confidentiality. When the information has been appropriately encrypted, we can assume that even if a threat actor were able to get a copy of that encrypted text, they can't decrypt and read it. That seems simple enough. However, the threat actor has an opportunity to steal a copy of the information either before it's encrypted or after it has been decrypted.

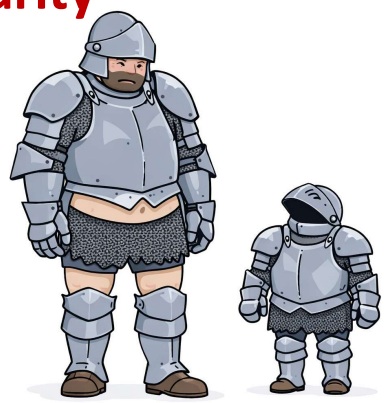
The other tactic a threat actor could employ is to steal the encryption keys used for encryption. The keys must be protected while also being usable. How do we protect an encryption key while also using it? For all of the solutions we have tried over time, there has yet to be an infallible way of doing that. And this will likely always be a struggle. If you do not know who has access to your encryption keys, then you do not know who has access to your data!

Truth #9

All good security is custom-fit

Compliance does not equal security

Compliance Is:
Old, Vague, a Low Bar, Watered Down
Passing The Audit Is Not Security
Attackers don't audit your systems,
they attack them!



This is one of the most misunderstood truths in our industry. Compliance frameworks are valuable; they provide structure, baseline expectations, and a shared language. But they are designed for *generality*, not precision. They aim to set a common floor, not build a tailored defense. Organizations that treat compliance as the end goal of security often end up with a false sense of safety—secure on paper, but still dangerously exposed.

Real security must be **custom-fit to the unique context of the organization**—its mission, risk appetite, culture, technology stack, and threat landscape. A hospital faces different risks than a financial firm. A small manufacturer cannot be secured in the same way as a cloud-native tech company. Yet, too often, security programs are built to "pass the audit" rather than protect what truly matters to the business. This leads to wasted resources, misaligned controls, and coverage gaps that attackers are more than happy to exploit.

Compliance tells you *what* to do, but rarely *how* to do it well. It won't tell you which applications matter most, where your most significant exposure lies, or how to align security with your business priorities. That requires a tailored approach—one that begins with understanding your specific environment and evolves with it over time. Effective security isn't about checking boxes. It's

about solving the right problems, in the right way, for your specific context.
In short, **compliance can support security, but it can never replace it**. Strong security adapts to your organization, not the other way around. Just like a tailored suit, it only works if it fits you.

One of the downfalls of compliance is that it implies an end game. Once we reach compliance, there's nothing else to do. Of course, this is wrong.

Sometimes being compliant can lead to undesirable outcomes. For example, the US government has compliance regulations called Federal Information Processing Standards (FIPS). It states that US "Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53," and includes systems managed by non-federal organizations that handle federal data that must meet these requirements.

These requirements include a vendor submitting their product to a NIST-approved lab for testing. The lab will test all components of the product before certifying that it is compliant. On the surface, this sounds like a positive step in ensuring security. But there can be unintended consequences.

A Commercial Off-The-Shelf (COTS) application may have an update released by the vendor that has new security features. Those might include fixes for known security issues that the older version of the application had that are currently being actively exploited. It is therefore important and time-critical to update as soon as possible. However, it takes time for NIST to review and certify the new version for FIPS compliance. The organization must now decide to update and address security and risk concerns to avoid being found out of compliance.

Truth #10

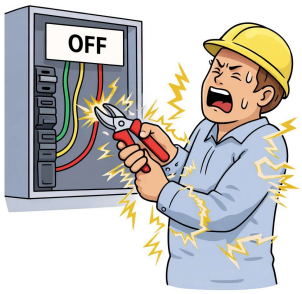
In security, the most dangerous thing in the world is what you think you know.

"There are known knowns. There are known unknowns. But there are also unknown unknowns. There are things we don't know we don't know." Donald Rumsfeld

Evidence Proves Events

No Evidence Proves Nothing

Do Not Assume - Verify



As Donald Rumsfeld once famously stated: "There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know." He went on to say that the unknown unknowns are the ones that concern him the most.

Absence of evidence is not evidence of absence. Just because we are not aware of something doesn't mean it doesn't exist. A practical example of this concept would be the following. If there is a log entry for a particular event, you are certain that that event has occurred. There is evidence that it did. For the sake of argument, let's now explore a scenario where there is no log entry for that event. Can we prove that the event didn't occur? Just because there is no entry doesn't mean the event didn't happen.

This speaks to the false confidence that often undermines even the most well-funded security programs. The belief that "we're secure," "we've got that covered," or "that system isn't exposed" creates blind spots—places we stop questioning, auditing, or improving. It's not ignorance that's most dangerous in cybersecurity—it's **assumed knowledge** that turns out to be wrong.

Breaches often don't happen because organizations had no security—they

happen because teams *thought* they had secured something. They believed patches were applied. They assumed logs were being collected. They trusted that users were trained. But when reality meets assumption, attackers find the gaps, and they exploit them without resistance.
This is why humility is one of the most powerful traits in a security team. **Assume you've missed something. Assume there's an unknown vulnerability. Assume the attacker is already inside.** That mindset leads to stronger validation, continuous testing, and more rigorous questioning of your environment. It drives red teaming, tabletop exercises, and risk reviews—not because you know you're insecure, but because you know you can't afford the luxury of overconfidence.
In this field, what you think you know can hurt you. What you *verify*, *test*, and *challenge*—that's where real security begins.

The same can be said about breaches. When we have evidence that a breach has transpired, we can quantify and qualify it. We can measure and prove that the event or events had in fact occurred. In other words, we can prove the breach.

In a scenario where we don't have evidence of a breach, does that mean that there is none? Or did we miss the evidence? Or was there a lack of evidence? How do you prove a negative? It is a very difficult proposition.

Truth #11

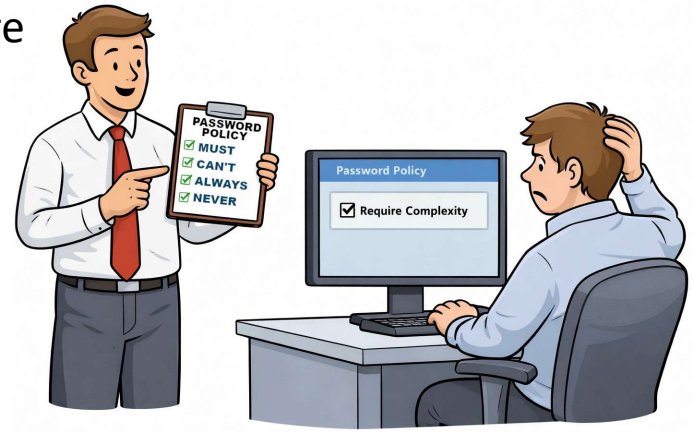
You cannot secure what you do not control

Defaults Are Not Secure

Software Has Bugs

Policy ≠ Control

Some Settings Cannot Be Changed



There are many different ways to apply this truth, but the fact is, we didn't design, manufacture, and program everything in our organization. Vendors of hardware and software do this heavy lifting for us, and then sell it to us in some state or form that we can, and typically will, modify for our customized use.

Well… Until we don't.

Defaults

The products to be secured in our environment are almost without fail insecure. And they are configured to be insecure on purpose. The default settings of these IT products, whether they're for networking, data handling, security, or whatever the functionality, are in a state of functionality.

Bugs

All of these products were designed by humans. Humans are fallible. We learned that in our discussion of Truth #4. Even as Artificial Intelligence (AI) starts designing and building more physical and logical designs, there will still be flaws. Because humans made AI.

Settings we can't change.

When it comes to the options and settings we can configure, we can typically only change what the vendor gives us the option to change. The one exception

is where we had full control over hardware or software. For example, open-source software. Like the Linux operating system. With open-source code, we can make our own changes to add or remove whatever we like. While that gives us more control, we are back at the bug problem. We can make mistakes that add vulnerabilities. And our chances of making and not finding those mistakes are greater as we don't have others trying to find our flaws. That brings us back to the issue of James Randi's, "If a man can make it, I can break it."

To recycle an old phrase from childhood. “You get what you get and you don’t throw a fit.” We are captive to the options the vendor has provided.

For those settings we can change, the cybersecurity team is likely not the one implementing the changes. One of the most challenging aspects of cybersecurity is attempting to manage the security settings of systems that the cybersecurity department doesn't control. Our jobs rely a lot on other people doing their jobs correctly. We can define it in policy. But that doesn’t mean the work is actually being done.

This principle is as foundational as it is overlooked. Security depends on visibility, authority, and influence—if you can't see it, manage it, or enforce policy over it, you can't protect it. Yet in today's environments, sprawling cloud services, unmanaged endpoints, shadow IT, and third-party vendors have expanded the attack surface far beyond what most security teams can fully govern.

Every asset that lies outside of your control—be it a cloud-hosted application configured by marketing, a third-party contractor's laptop, or a vendor API—becomes a potential breach point. And if you don't have the ability to audit, patch, monitor, or contain it, you're left hoping nothing goes wrong. Hope is not a security strategy.

This concept is especially important in the era of distributed work and complex supply chains. It forces a shift in thinking: security isn't just about defending the perimeter—it's about establishing **zones of control** and making hard decisions about what falls inside those zones. If you can't control something, you must at least account for the risk it introduces and decide how to mitigate or isolate it.

Ultimately, **control defines the boundary of responsibility**. Security teams are held accountable for incidents, but unless they are also empowered with control over systems, tools, and architecture, they're set up to fail. If we expect security to work, we must first ensure that the people tasked with protecting the organization have the authority and access to do so effectively.

Truth #12

You cannot prevent what you allow

Access Enables Attackers

Every Allowed Path
is a Potential Attack Path

Permissions Create Exposure

Allowed Access Is Also Attacker Access

This statement strikes at the heart of one of security's most persistent contradictions: granting broad access or making security exceptions while expecting airtight prevention. If a system, user, or process is authorized—even loosely—to perform an action, access data, or connect to critical infrastructure, then by definition, you have *allowed* that potential pathway for compromise. And you can't prevent what you've already sanctioned.

This is why misconfigured permissions, excessive privileges, and "temporary" access exceptions are some of the most common root causes of breaches. We allow too much, too often, for too long—usually in the name of productivity or convenience. And then we act surprised when that permission becomes the attacker's point of entry.

This truth reinforces the need for the **principle of least privilege**, **zero trust architecture**, and strong access governance. Prevention isn't just about blocking the bad guys—it's about **not enabling the conditions** that make exploitation possible in the first place. If we allow unrestricted admin access, insecure APIs, or third-party connections without oversight, we've already made the attacker's job easier.

Security must start with intentional boundaries. Every exception you make,

every access you allow, every policy you relax must be treated as a conscious tradeoff. Because once it's allowed—either by design or by neglect—you can no longer claim to be preventing it.

While this concept might strike the reader as odd or perhaps elicit a "no duh" response, it is a very important concept that is largely misunderstood. Take a lock on a door, for example. What is the purpose of the lock? While the typical response is, "to keep people out that shouldn't be there" or "to keep honest people honest", it can be argued that they are viewing the situation at the wrong angle.

The functionality of the lock is that it lets people in, not keeps them out. Because if we didn't need to allow people in, we wouldn't need the door. To keep people out, we would put up a wall instead of a door. Said differently, the lock allows the right people in. That is the function of the lock.

Looking at this in a different light, we can challenge how we view the problem. Let's examine a quote from Gene Spafford of NIST. He once said, “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts." While his sentiment is focused on securing the system, the important point is that the system itself is unusable. This would affect the availability of the CIA Triad. Therefore, it cannot be considered secure. We must allow access to the system and/or the data on it for the Availability vector of the CIA Triad.

Now let’s apply that notion to our network. Just like the lock, our network firewalls are allowing access. If I didn’t need to allow access from one network to another, I wouldn't need a firewall. I would simply unplug the network cable, making the network "air gapped". A firewall is simply a network router with a filtering ruleset. Routers are networking appliances that facilitate network communication. Most of the rules on that firewall allow network traffic based on known good uses. For example, a firewall may have a rule that allows access from an untrusted network (like the internet) to your web servers.

When we allow users from the internet to access our web servers, which is what we want, we cannot prevent adversaries from getting to that same server. Using technological parlance, if we allow TCP ports 80 and 443 traffic inbound from the internet into our DMZ, that means bad actors can access ports 80 and 443 from the internet as well. The firewall must allow that.

Truth #13

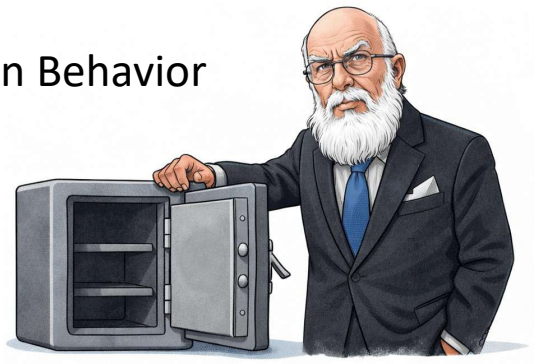
Security is, first and foremost, a people issue

"If a man can make it, I can break it."
The Amazing Randi

Most Breaches Begin With Human Behavior

Technology Enables,
but People Decide

Security Culture Matters Most



While we often focus on firewalls, encryption, and threat intelligence feeds, the truth is that most breaches begin—and sometimes end—with human behavior. People click links, reuse passwords, misconfigure systems, ignore warnings, or make decisions under pressure. Technology may enable the threat, but people are almost always the vector.

This isn't about blaming users; it's about recognizing reality. Security culture, awareness, training, and leadership support are far more impactful over the long term than any single tool. An organization that invests in its people—educating them, empowering them, and building a culture of shared responsibility—will always be more resilient than one that relies solely on automation or technical controls.

Even the most sophisticated tools require human decisions: which alerts to investigate, which risks to prioritize, which controls to implement. And when something goes wrong—as it inevitably will—it's people who detect, contain, respond, and recover. Security succeeds or fails on the strength of the humans behind it.

In short, **technology may scale security, but people define it.** If you don't invest in your people through clear communication, accountability, training, and

support, your security program will always be incomplete, no matter how advanced your tools are.

It would be easy to write an entire book on all of the ways this truth affects our security. But for the sake of making this point, we will focus on what is likely to be the most important and likely the most critical aspects of this truth for most organizations. That aspect is social engineering.

People make mistakes. There is no other way around this. To compound the fact that they make mistakes, people also tend to err on the side of being helpful to their fellow humans. This desire to help others, coupled with our fallibility, is what bad actors take advantage of in social engineering attacks. The most prolific modern social engineers like Frank Abignail and Kevin Mitnick enabled their lives of crime by convincing people to do things they would not otherwise have done in order to bypass largely technical safeguards that were in place to prevent their access.

Another way that this concept can be expressed is in the maturity of the management of the systems. Some organizations have a much better grasp on their processes, system configurations, monitoring, etc., than others. If the organization isn't very mature in its execution, it is going to be harder to ensure any level of security. While one way we can alleviate some of this is through automation, more often than not, organizations that don't have strong people-led processes also lack the ability to automate.

James Randi, also known as The Amazing Randi, was a magician for his entire life. He was very good at it, and people started believing he possessed special powers. This made him very uncomfortable. He decided not to perform magic that would fool people into believing something that isn't real. What that means is he refused to lie and tell his audience that he had special powers that only he possessed. They were just illusions. He had found it to be unethical to fool people without their consent.

There were others who claimed that they did, in fact, have special paranormal or supernatural powers. They claimed to have powers such as bending objects without touching them, reading people's minds, or seeing through opaque objects. Randi decided later in his career to do something about it. He offered a challenge to anyone who claimed to have these special powers to fool him. If someone could perform actual magic that Randi could not debunk, he would award them a prize, which was at one time over one million dollars. Many people would try, but nobody would ever collect the award. Randi would reveal every single one of them as a scam.

Randi would say, “If a man can make it, I can break it.” And he’s not the only one.

The lesson for us in cybersecurity is that there is nothing we build that can't be broken. We can translate that sentiment into our IT assets and the organization itself. In other words, any security implemented by a human can be defeated by a human.

Truth #14

Some things cannot be fixed

They are simply reality

Some Risks Cannot Be Eliminated

Attacks always get better;
they never get worse. - Steve Gibson

What if the solution is worse than the problem?

This final truth gives us a natural conclusion to the other thirteen. We must acknowledge that there will be residual risk. There are some risks that simply cannot be mitigated. For example, by having our systems connected to the internet, they can be reached by others on the internet, including those who want to do us harm. The only remedy is to remove the systems from the internet, which is something we cannot do because we need those systems to be reachable by others on the internet.

This concept can also be framed by the saying, “the solution is worse than the problem.” Most systems and data can be secured to an acceptable level IF we disregard the expense of resources in doing so. However, in real-world scenarios, we would not consider expending the resources it would take to secure said assets.

Sometimes the problem is that not all parties can agree on the solution, even if all parties agree on the problem. When that happens, someone is going to be upset that their ideas were not properly taken into account. This fact of life needs to be acknowledged. The best solution will not always receive 100% agreement. It doesn't mean it's not the right thing to do. There is wisdom in the saying: If all parties are equally unhappy, you've probably arrived at the solution.

Our defensive measures always lag behind the offensive plan. Since defense is always in reaction to the offense, the defense simply has the advantage of acting first.

This quote resonates deeply in the world of cybersecurity, where so many of our so-called "problems" are, in truth, enduring conditions of the digital landscape. We treat breaches as failures, zero-days as crises, and human error as something to eliminate—when in fact, these are not problems to be solved once and for all, but **realities to be managed continuously**.

Attackers will always evolve. Users will always make mistakes. Systems will always have vulnerabilities. If we approach these facts as problems to fix permanently, we will spend our careers chasing illusions of control. But when we reframe them as **persistent conditions**—as part of the environment we operate in—we stop searching for silver bullets and start building systems designed to *live with and adapt to* risk.

This mindset shift is liberating. It moves us from trying to eliminate every threat to **managing exposure, reducing impact, and recovering quickly**. We stop asking, "How do we prevent all phishing?" and start asking, "How do we detect and contain the phish that gets through?" We stop demanding perfection from users and start designing systems that expect failure but don't collapse under it.

In cybersecurity, not every problem has a solution. But every reality can be addressed with resilience, strategy, and humility. That's how we evolve from a reactive discipline to a mature, adaptive one.

Join Us!

Workshop: How to Think Like a Cybersecurity Defender

Friday, April 17th

12-4 pm US Eastern Time

www.antisyphontraining.com