NEW AMERICA

Dan Ward

CYBERSECURITY, SIMPLICITY, AND COMPLEXITY

The Graphic Guide to Making Systems More Secure Without Making Them Worse

March 2016

About the Author

Dan Ward is the author of *The Simplicity Cycle: A Field Guide To Making Things Better Without Making Them Worse* (HarperBusiness, 2015) and *F.I.R.E.: How Fast, Inexpensive, Restrained and Elegant Methods Ignite Innovation* (HarperBusiness, 2014).

Prior to launching Dan Ward Consulting, he served as an acquisition officer in the US Air Force, where he specialized in leading high-speed, low-cost technology development programs and retired at the rank of Lieutenant Colonel.

Dan's expertise on defense acquisition reform has been featured in publications from the White House, the U.S. Senate and the British Parliament. His writings have also appeared in outlets including Fast Company, Forbes, The Boston Globe, Armed Forces Journal, and Small Wars Journal.

Dan holds three engineering degrees and received the Bronze Star Medal for his service at NATO Headquarters in Afghanistan leading an international team of officers from five different countries. He lives in Massachusetts with his wife and two children.

About the Artist

Hannah White is a D.C.-based designer and illustrator. She studied digital design at the George Washington University through the Corcoran College of Art and Design.

Acknowledgements

Bruce Schneier for generously agreeing to talk with me.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

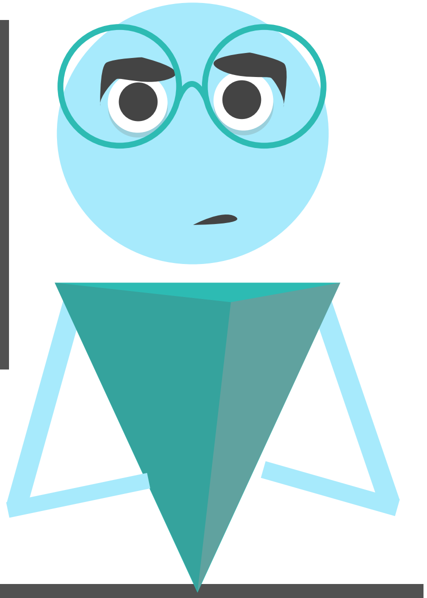
The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work—for the countries, for companies, and for individuals.

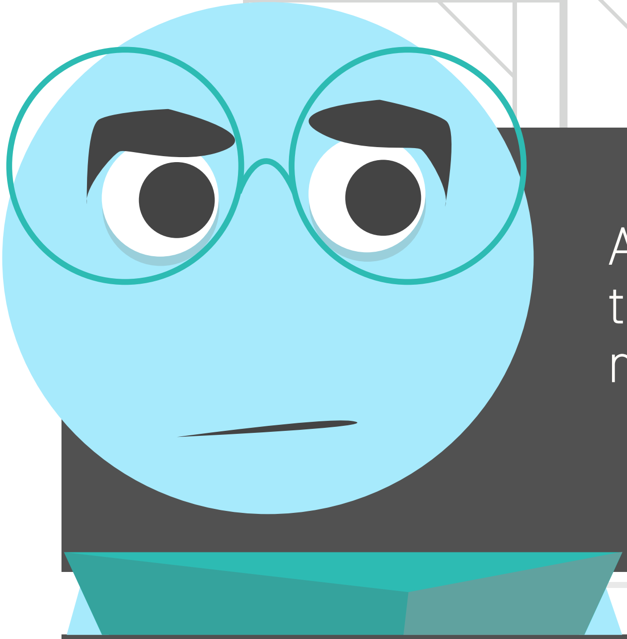
Find out more at **newamerica.org/cybersecurity-initiative**.

Let’s talk about

cybersecurity.

Specifically, let’s look at the way **complexity** affects the **vulnerability** of cyber-systems.





As we’ll see, simplifying things can make our system more **secure.**

Note that I didn’t say *perfect.*

Why does complexity in cyberspace matter?

Take this short quiz to find out.

Complexity is

A. Increasing

B. Inevitable

C. Unavoidable

D. A pretty big problem

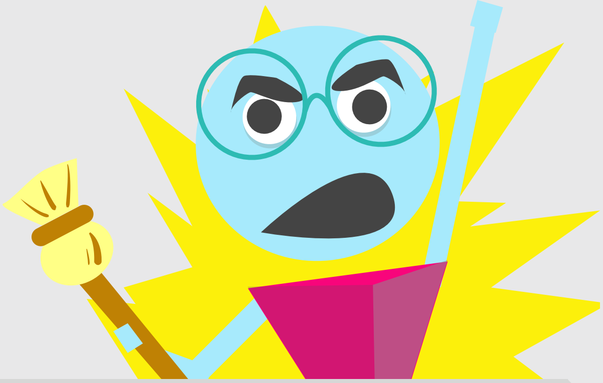
[✓ E. All of the above]

People have all sorts of crazy ideas about

simplicity.

Some people love it too much...

Simplify all the things!



...While others don't trust it at all.

Simplicity?

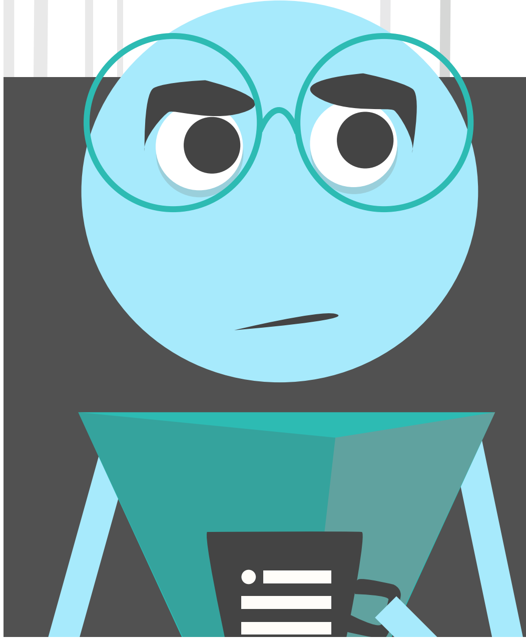
I fear simplicity.

Black Hat founder Jeff Moss argues for Radical Simplicity in cyber-systems, which involves stripping away excess functions from critical systems to protect core processes.

In contrast, GRT Corp says “We must embrace complexity to improve cybersecurity.” According to them, complexity fosters security.

And way back in 1999,
Bruce Schneier wrote:

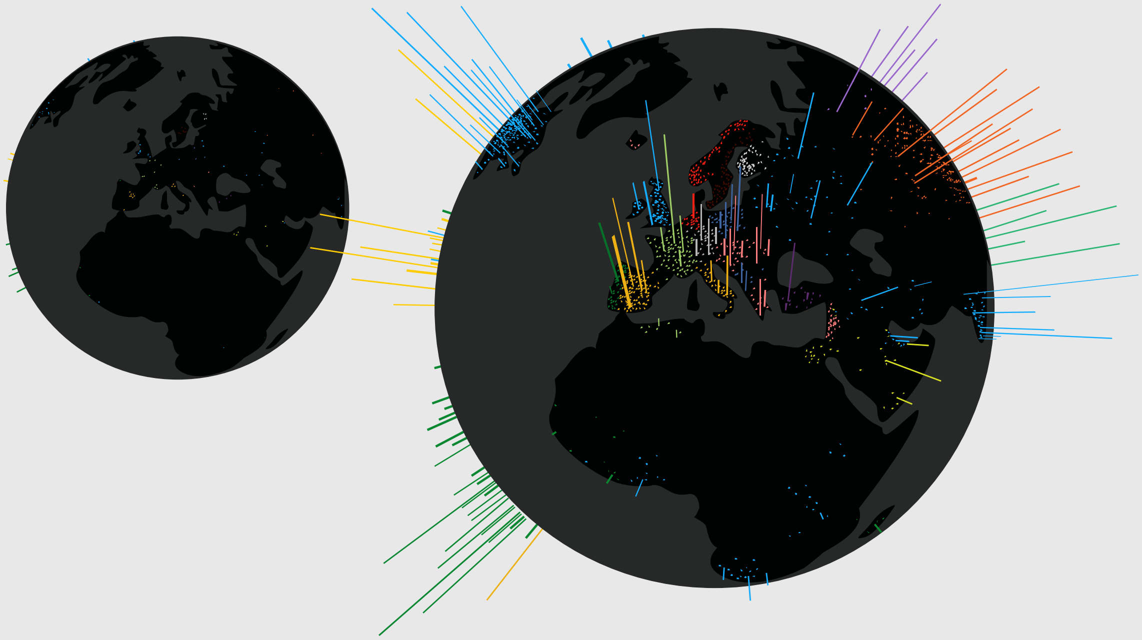
“The worst enemy of security is complexity.”



**So who is right?
Schneier, of course.
That guy is brilliant.**

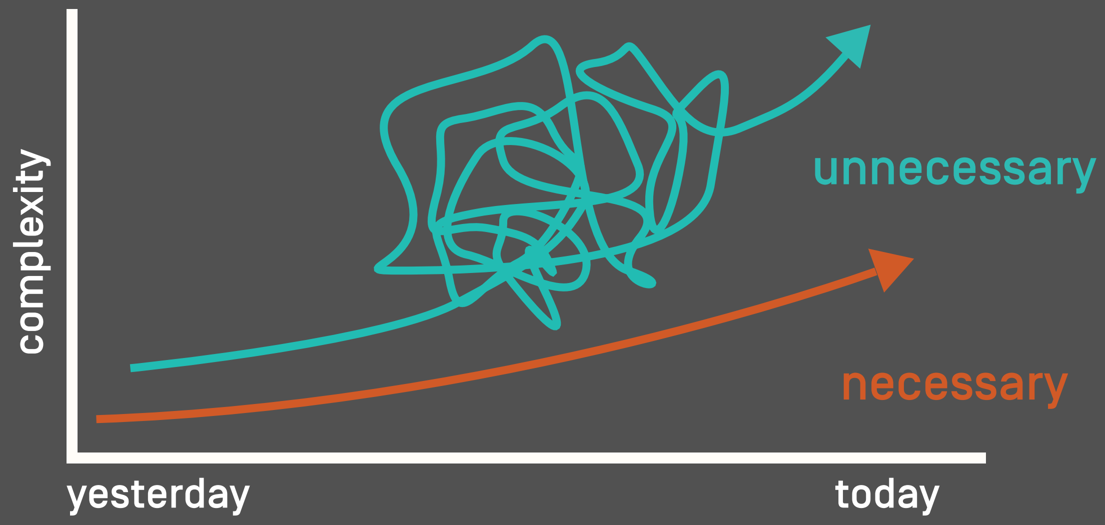
But Team Complexity has a point too. See, cyberspace is a complex place... tool...network...er, thing. And it’s getting more complex everyday.

What started out as a small group of loosely connected machines that performed a few functions is now a vast network of deeply intertwingled nodes that does almost everything.



“The networks of the future will be necessarily more complex, and therefore less secure.” Schneier, 1999

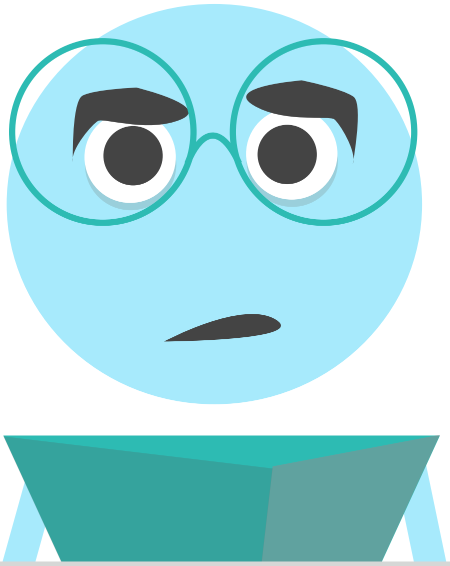
And don’t get me started on the whole Internet of Things! So let’s not pretend this stuff can ever be simple. But while today’s level of necessary complexity is higher than yesterday’s, just like Schneier predicted...



...there's plenty of unnecessary complexity out there, and it's only increased over time. That represents a pretty big opportunity for improvement. The idea is to minimize unnecessary complexity.

Complexity reduces security in several ways. First, complexity makes vulnerabilities harder for developers and testers to uncover. Each feature, function, and interaction is a potential **threat vector.**

The more pieces, the more time and effort is required to test them all.



It’s the proverbial needle in the haystack!

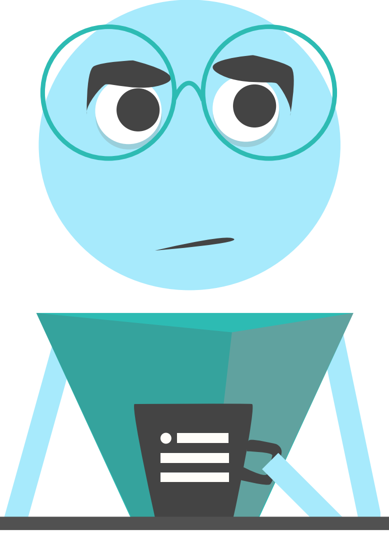
hay3

needle

hay2

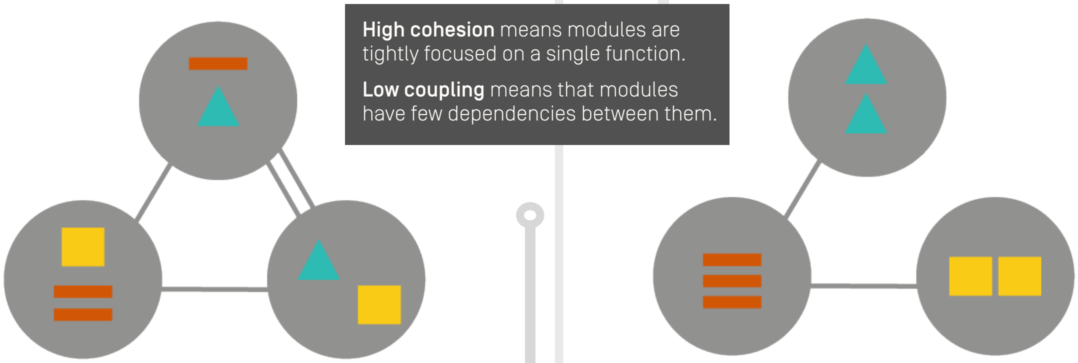
hay1

...or C++ stack, in our case.



Second, complexity makes vulnerabilities **harder to fix** once we find them.

Particularly if the system in question violates the “high cohesion/low coupling” principle. Excessively complicated systems usually do, so flaws in one area ripple through the rest of the system.



High cohesion means modules are tightly focused on a single function.

Low coupling means that modules have few dependencies between them.

Low cohesion / high coupling:
This structure is not secure and difficult to debug.

High cohesion / low coupling:
This structure is more secure and easier to debug.

But worst of all, complexity creates the illusion of security.

That can be an expensive and dangerous illusion to maintain. When we think our systems are more secure than they actually are...

...we're setting ourselves up for some nasty surprises.

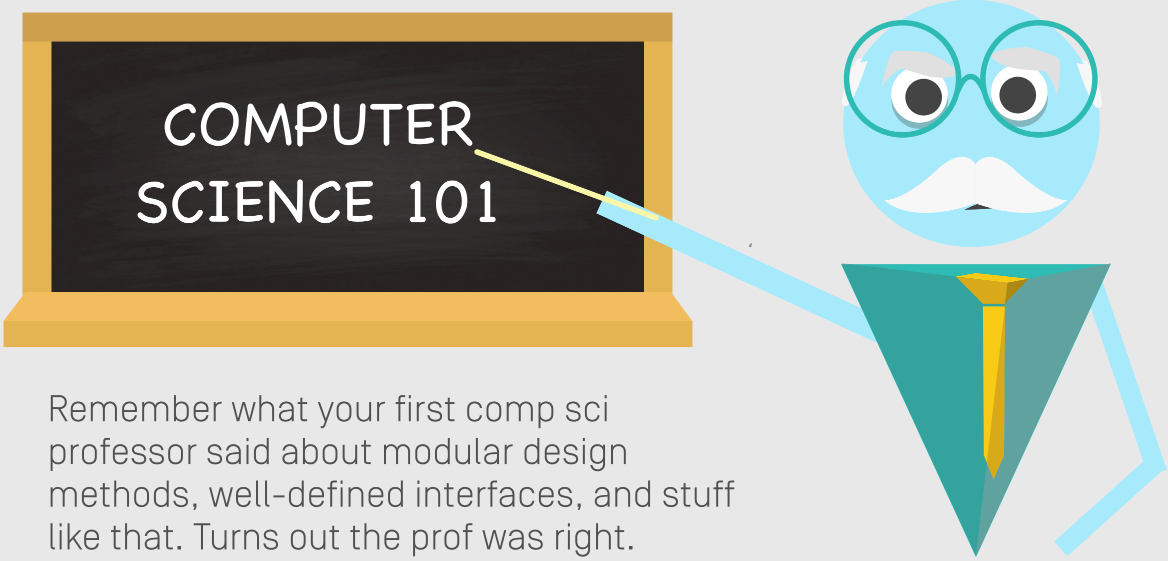
Read any issue of *2600 Magazine* for proof of that.

Ok, wait a minute. Didn't that quiz on page one say that complexity is **inevitable?** Sounds like we don't have an option!

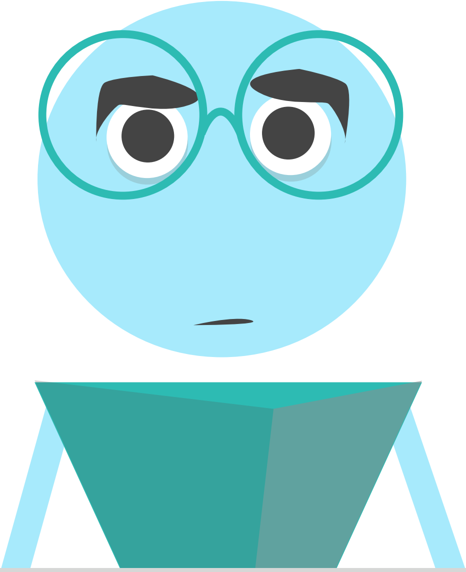
Good news!

We have an option.

For all of my fellow coders:



Remember what your first comp sci professor said about modular design methods, well-defined interfaces, and stuff like that. Turns out the prof was right.



Not a coder? Not a problem!

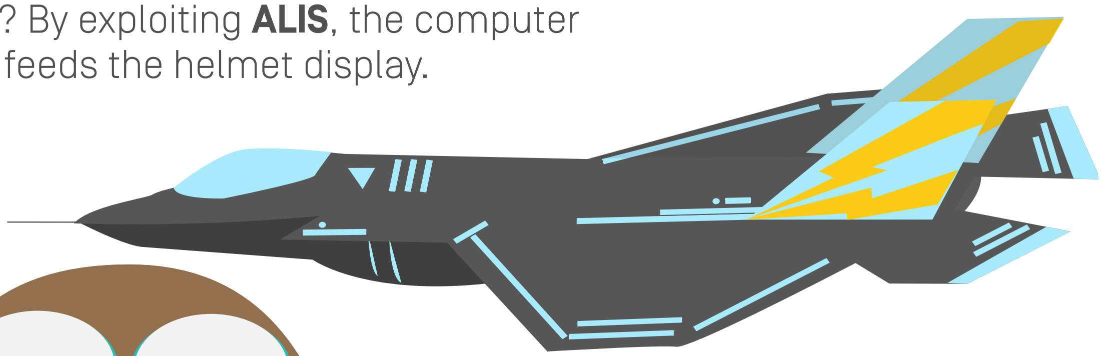
Well-informed **consumers** can insist on this. So can CIO's and policymakers and think tanks.

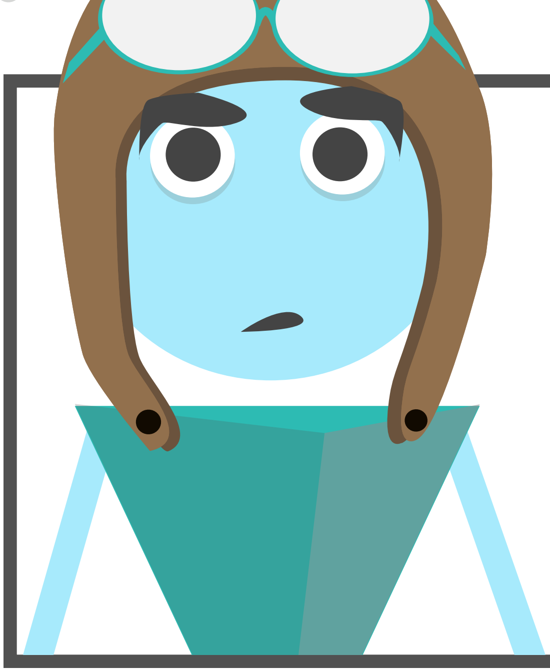
And me of course. We all have a role to play.

This isn't just about IT systems. Cyber vulnerabilities can also affect hardware.

Like a F-35 Fighter Joint Strike Fighter Jet, for example. A pretty scary article described a scenario where the F-35 could be taken down without a single shot fired.

How? By exploiting **ALIS**, the computer that feeds the helmet display.

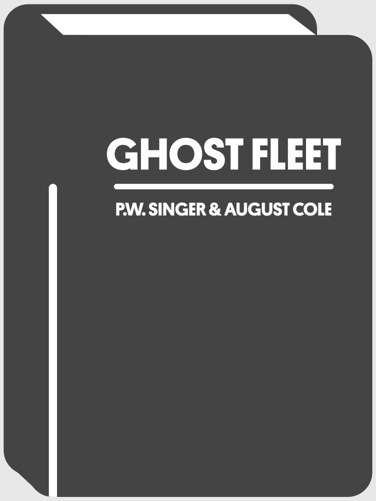




A hacker could theoretically **brick the jet**—or the entire fleet—through ALIS.

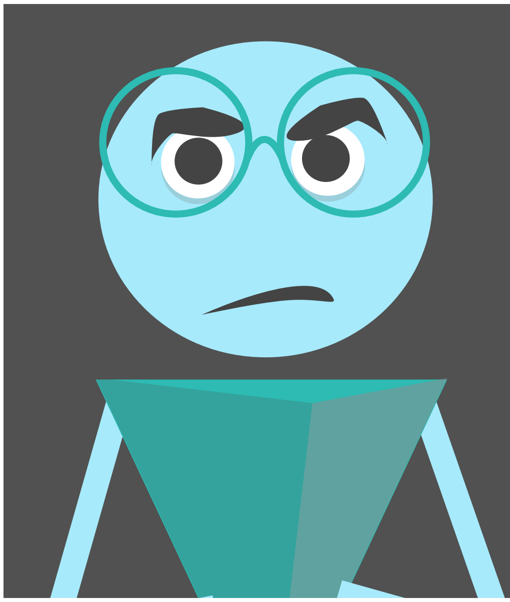
And that's only one potential threat vector. The F-35 relies on nearly 30 million lines of code. With that much complexity comes a lot of hidden vulnerabilities.

In the recent novel *Ghost Fleet*, hacked computer chips render the JSF useless in combat. Sure, it's fiction, but it's really well-researched fiction.



I hope you see there are some steps we need to take to generate improvement. There are technical steps we can take to make technology more secure. Dan Kruger, founder of Absio, has one suggection:

> "Cybersecurity is radically simplified if we move primary information security into the information itself."



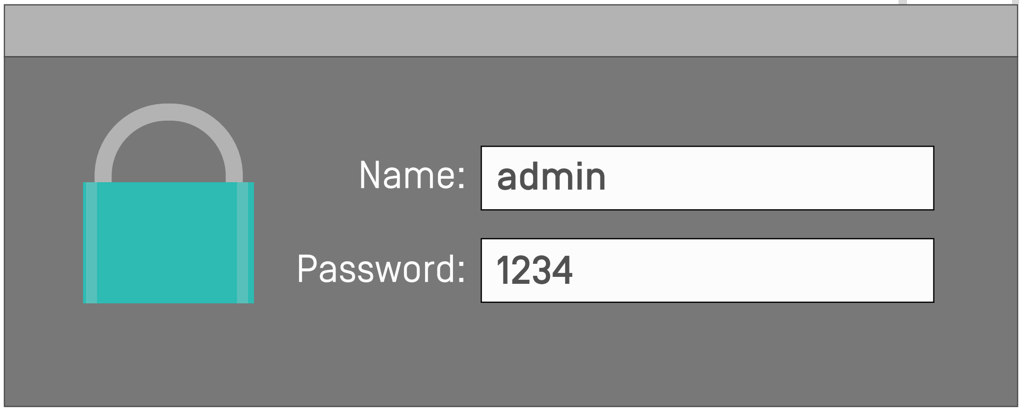
That reduces the number of useful attack vectors and "ruins the economics of hacking."

There are also procedures we could follow. Like, people should stop using "1234" as their password.

Quit doing that, people.

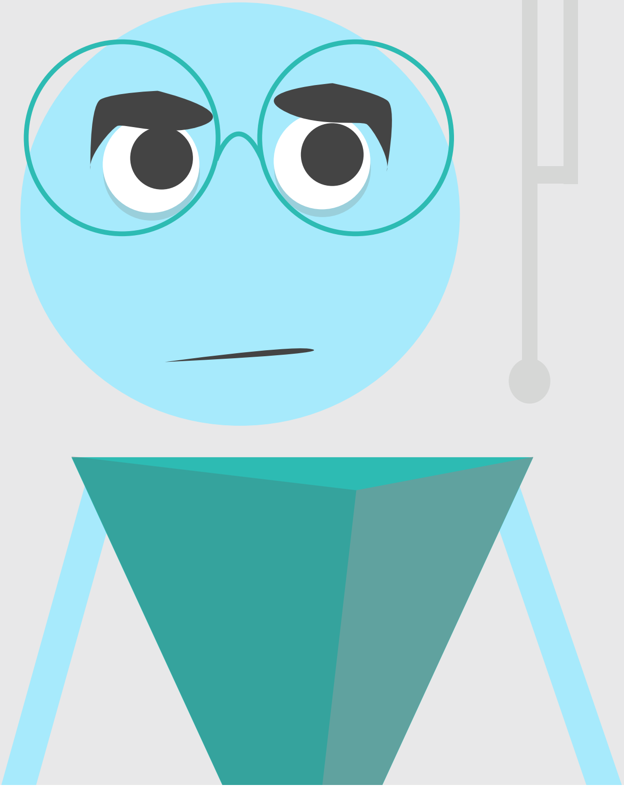
Shodan, a search engine for the Internet of Things, shows that lots of important systems ***retain their default login and password.***

We’re talking power plants, medical devices, traffic control systems, and security cameras.



Name: admin

Password: 1234



In a world of Internet complexity, dumb passwords can create huge vulnerabilities.

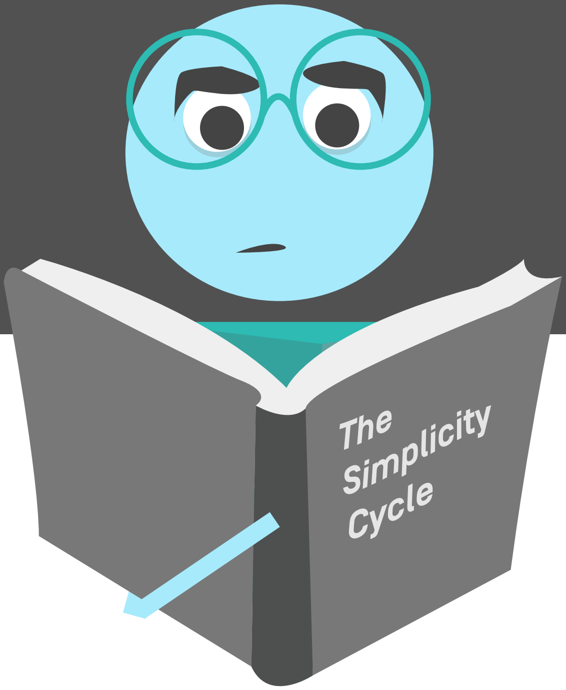
Fixing the “1234 vulnerability” is as easy as hard-coding a first-use password reset requirement.

It’s not a sexy fix—simplicity seldom is—but it would be a great first step. Still, the core issue is that we need to make better decisions.

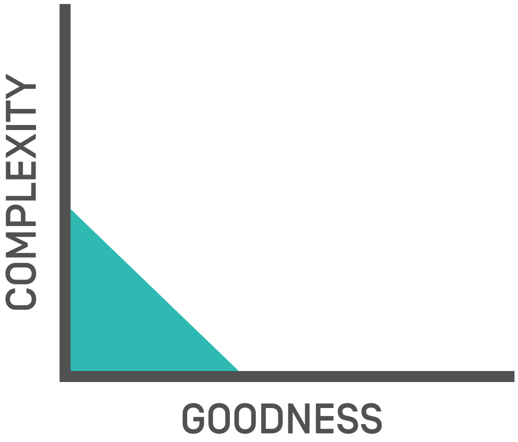
Good news—there is a book where you can read all about how to make better decisions when it comes to complexity!

It's called *The Simplicity Cycle.* The book explores the relationship between complexity and goodness in a wide range of situations.

In this context, "goodness" means security.



The goal is to highlight ways to make things better...without making them **worse.**

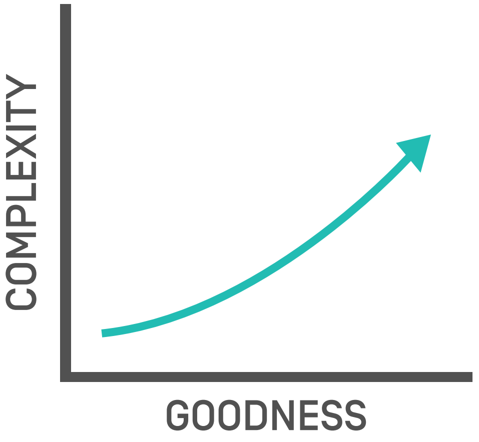


For example, the early ARPANET protocols were all about openness, not security.

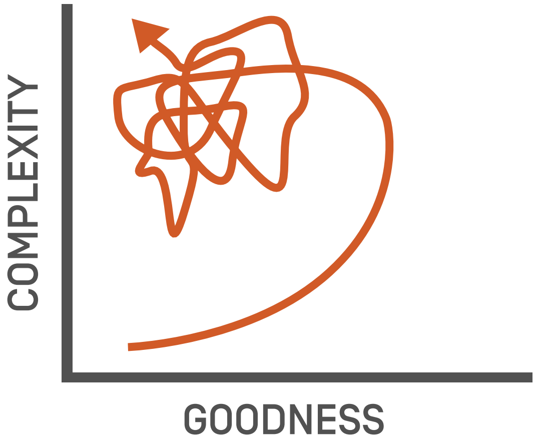
That puts us in the lower left corner of the chart. Down there, complexity is low, and so is security.

As the Internet grew, security started to matter.

So we added passwords, encryption, and VPNs. Things got **more complex** and **more secure.**

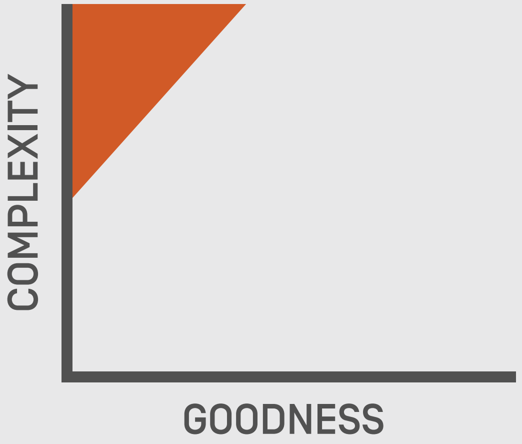


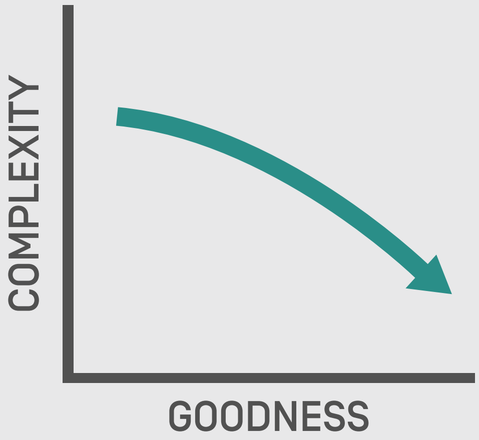
That was OK for a while. But if we're not careful, increased complexity will make things worse!



In this area, people tend to make loopholes and backdoors...or they just don't use the system.

The result is essentially a **self-inflicted denial-of-service-attack.** Not OK!



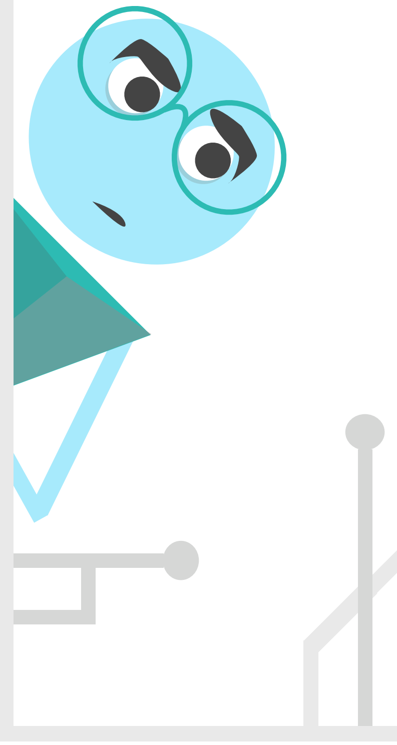


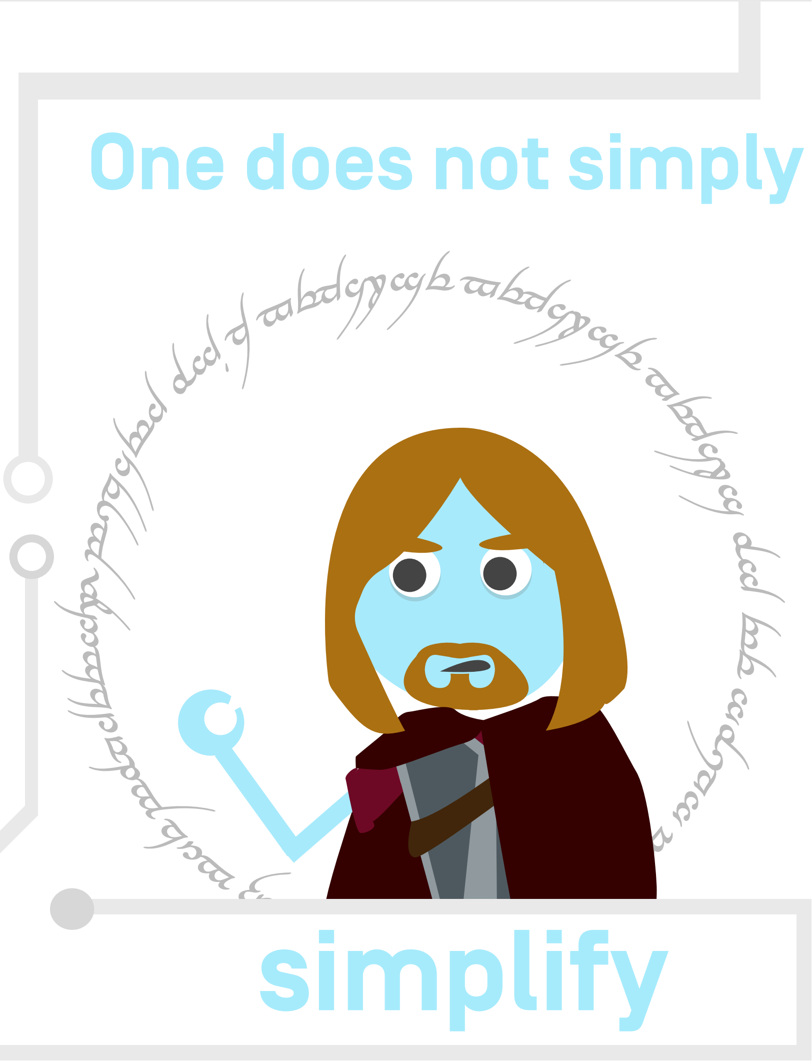
Fortunately, there's a better alternative. Instead of continuing to add complexity...

...at a certain point, the way to make things better is to make them simpler.

Easier said than done, I know.

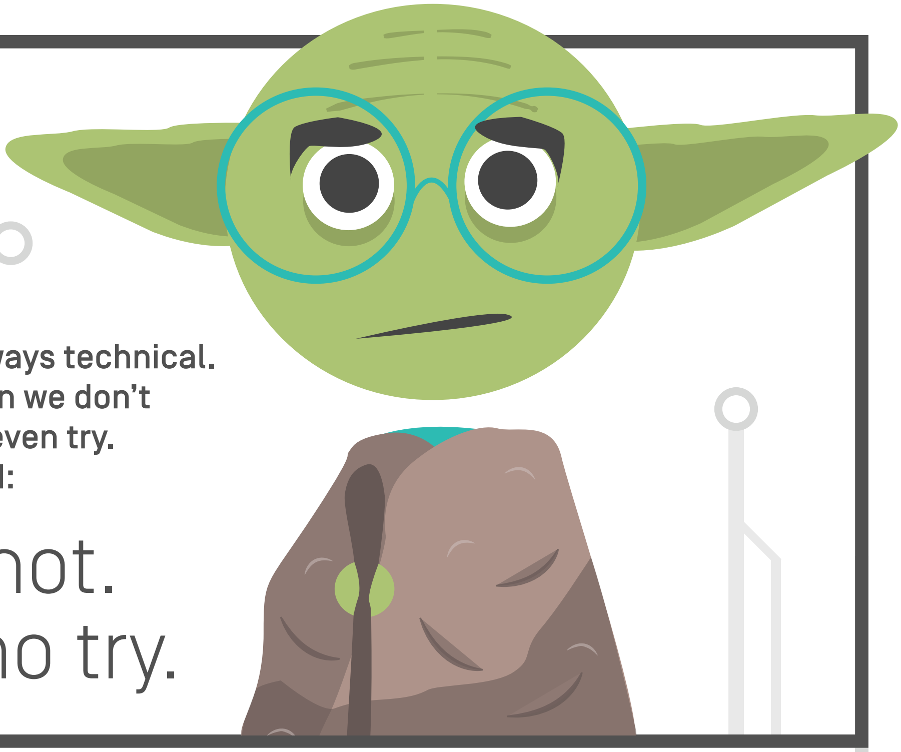
But why is it so hard to make things simple?





The difficulty isn't always technical. Sometimes the reason we don't do it is that we don't even try. But as Yoda once said:

Do or do not.
There is no try.



In all seriousness though, the challenge of simplifying is often more cultural than anything else. We treat complexity as a sign of **sophistication**, a desirable attribute of our systems. We know how to simplify. But we choose not to.

too much
too little
COMPLEXITY
GOODNESS

We even brag about our 30 million lines of code, as if complexity and goodness are the same thing.

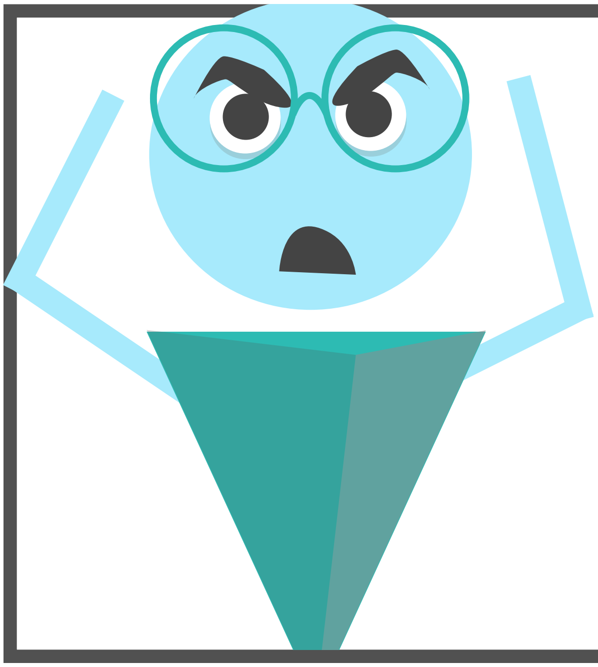
But as we've seen, too much complexity can be just as bad as too little.

But yes, sometimes simplicity can be difficult to achieve.

Simplification requires restraint.

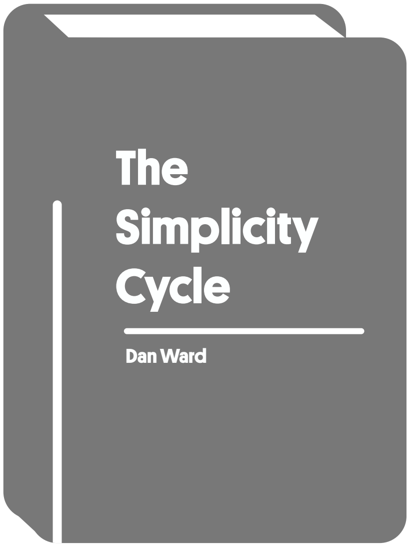
Doing less...

...and making judgements about what to add, what to retain, and what to discard.



We fear making the wrong decision, deleting something important.

...or we get too attached to our pet feature, or the latest trend, so we end up adding too much and keeping everything!

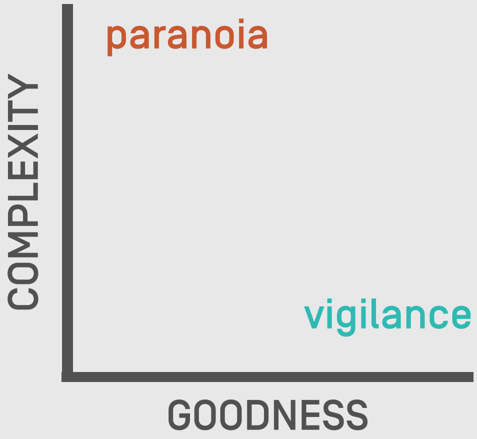


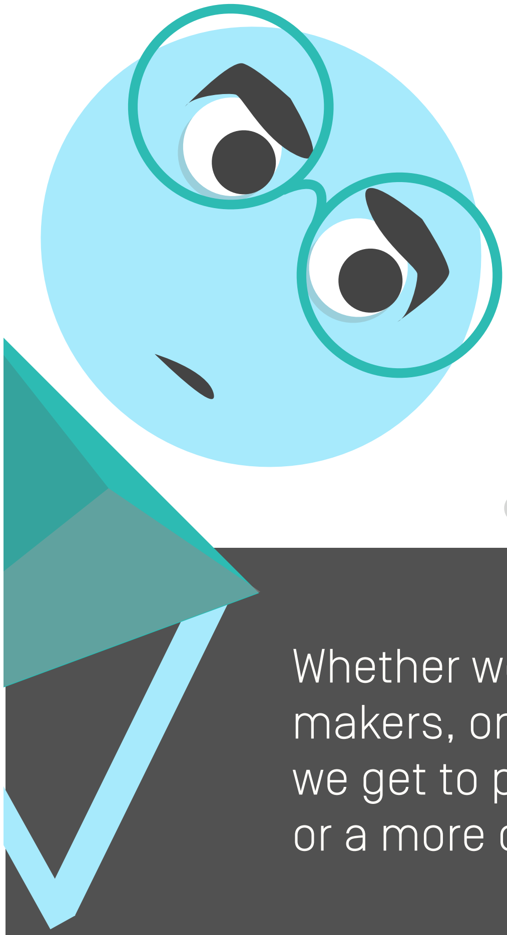
That’s where *The Simplicity Cycle* comes in.

It provides a framework to help us have difficult discussions about complexity, so we can understand the actual costs and benefits.

When we’re talking about security, it helps us distinguish between vigilance and paranoia.

It introduces tools and techniques that orient our designs towards ideal solutions, which are simple and good.





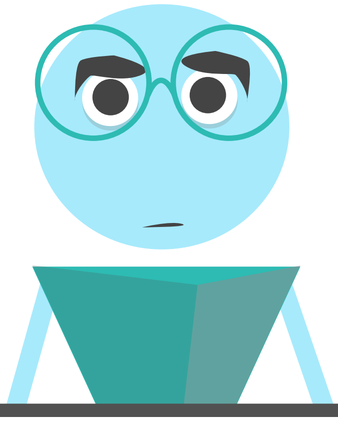
That's really the key. We always have simpler alternatives to choose from.

Always.

Whether we are designers, coders, policy makers, or users, if we're making decisions, we get to pick between a simpler approach or a more complex one.

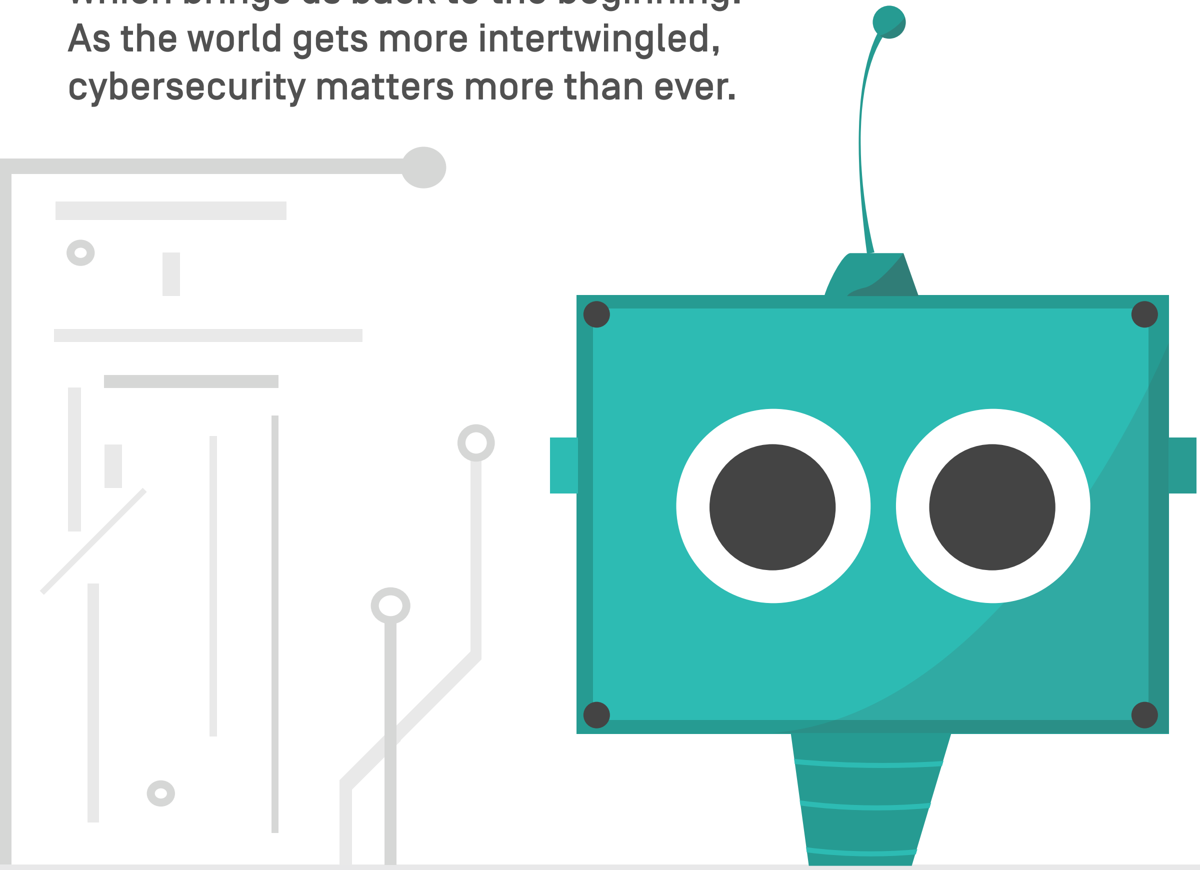
I'm not saying simpler is always better...

...just that simpler is always an option... and it's worth considering.



Solutions that are simple and effective may be difficult to find at times, but they're much easier to find if we actually look for them.

Which brings us back to the beginning: As the world gets more intertwingled, cybersecurity matters more than ever.



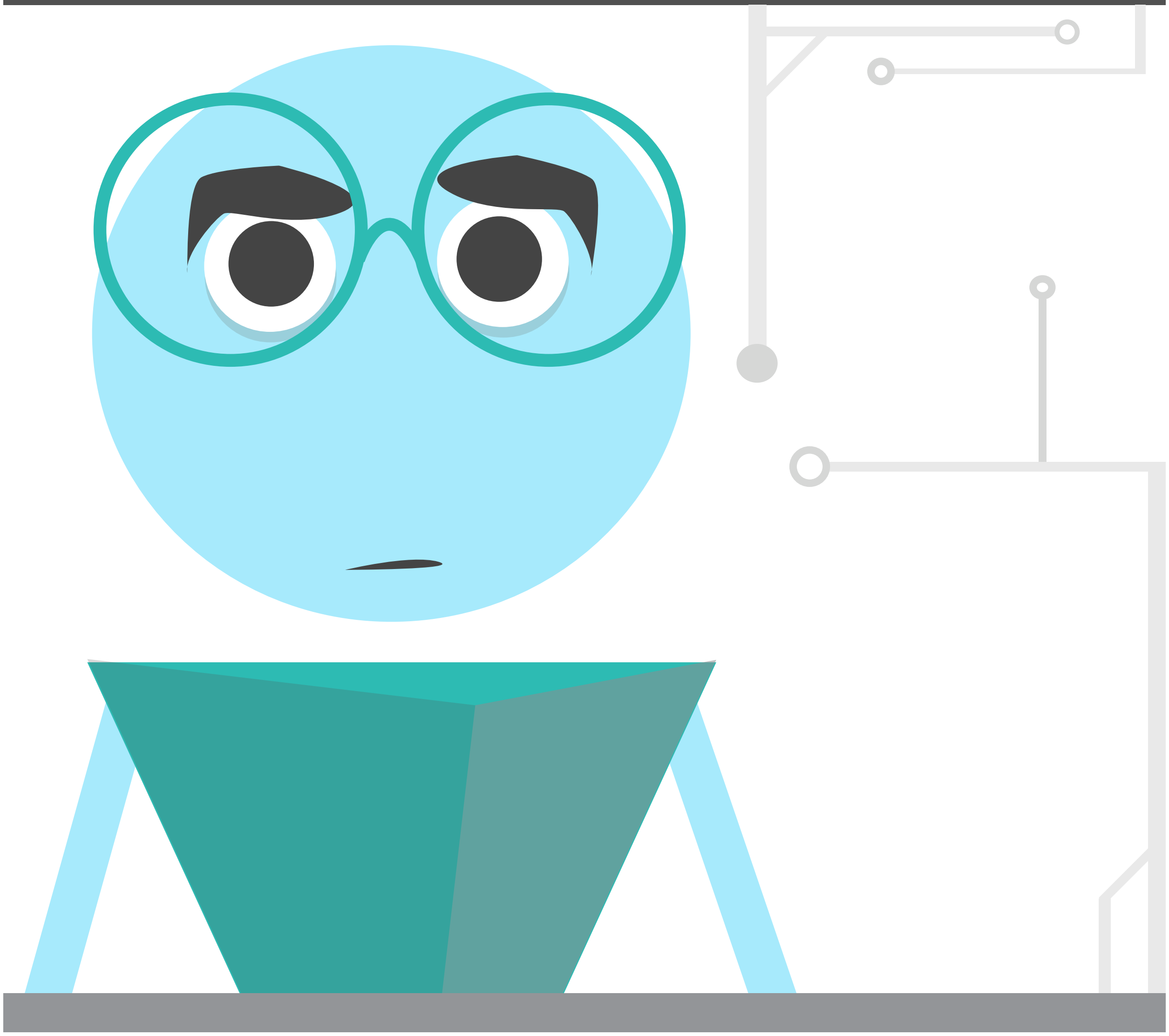
It affects fighter pilots and bankers and merchants. It even affects people who have no idea who Mr. Robot* is.

**Mr. Robot is a great show that you should watch.*

So whether you're writing code or writing policy, or just writing emails, watch out for unecessary complexity.

Take a moment to consider whether a simpler approach might be more effective.

Our cybersecurity depends on it!



REFERENCES

1 To Improve Cyber-Security We Must Embrace Complexity. GRT. http://www.grtcorp.com/content/improve-cyber-security-we-must-embrace-complexity.

2 Meyer, Claire. “The Hunt for Cybersecurity Solutions at Black Hat 2014.” Security Magazine. http://www.securitymagazine.com/articles/85863-the-hunt-for-cybersecurity-solutions-at-black-hat-2014.

3 Schneier, Bruce. “A Plea for Simplicity: You can’t secure what you don’t understand.” Schneier on Security. https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

4 Bender, Jeremy. “The New F-35 Fighter Jet Can Be taken Down Without A Bullet Ever Being Fired.” Business Insider. http://www.businessinsider.com/f-35-hackers-2014-2

5 Leaked F-35 REport Confirms Serious Air Combat Deficiencies. Pogo. http://www.pogo.org/our-work/straus-military-reform-project/weapons/2015/leaked-f-35-report-confirms-deficiencies.html

6 https://www.absio.com/sites/default/files/pdfs/Radically_Simplifying_Cybersecurity_V1.4.pdf

7 Goldman, David. “ Shodan: The Scariest Search Engine on the Internet.” CNN Money. http://money.cnn.com/2013/04/08/technology/security/shodan/

8 Ward, Dan. *The Simplicity Cycle: A Field Guide to Making Things Better Without Making Them Worse.* Amazon. http://www.amazon.com/Simplicity-Cycle-Making-Things-Without/dp/0062301977/

9 Internet History. -Softheap. http://www.softheap.com/internet/internet-history.html