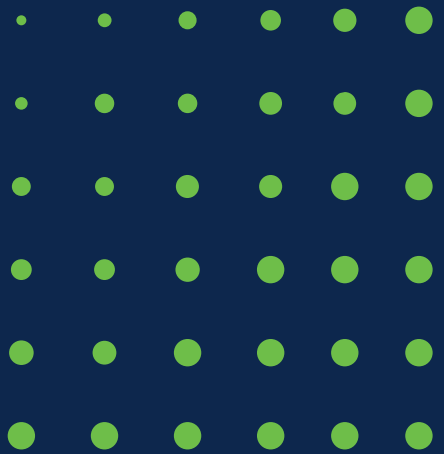
CISCO
SECURE

CISCO The bridge to possible

What Do We Owe One Another In the Cybersecurity Ecosystem?

Wendy Nather
Head of Advisory CISOs, Cisco
@wendynather

Not just “what can we volunteer to do” or “what would be nice,” but what do we owe?



Businesses are competing as ecosystems

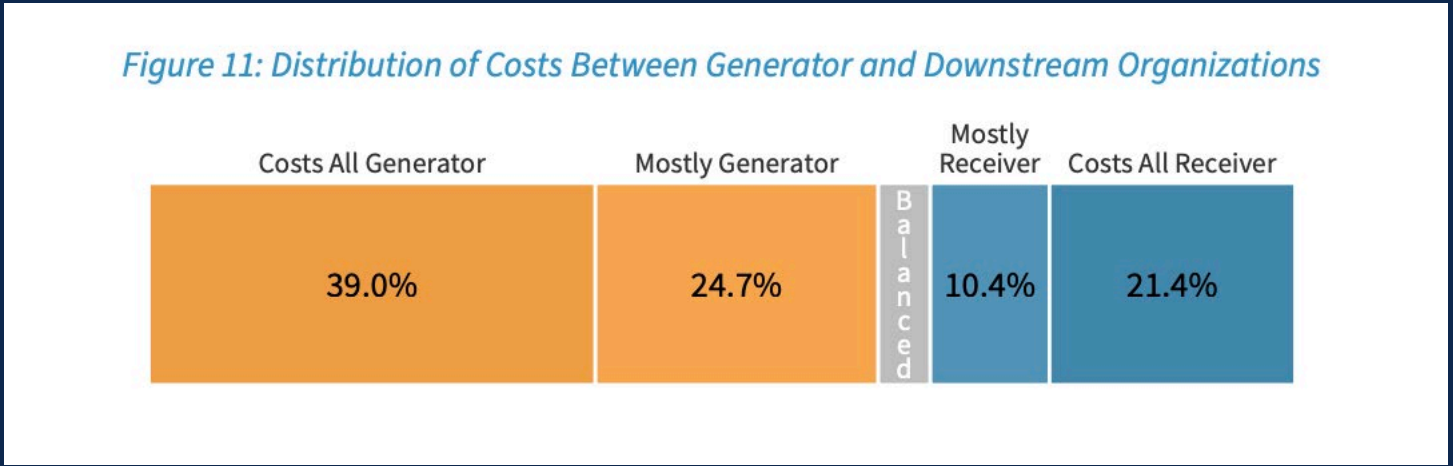
It’s no longer a matter of outrunning the other hitchhiker …

There’s more than enough bear to go around.

Breaches affect more than just the target organization

- The 2020 ransomware attack on BlackBaud affected 800 different organizations, including nonprofits and healthcare

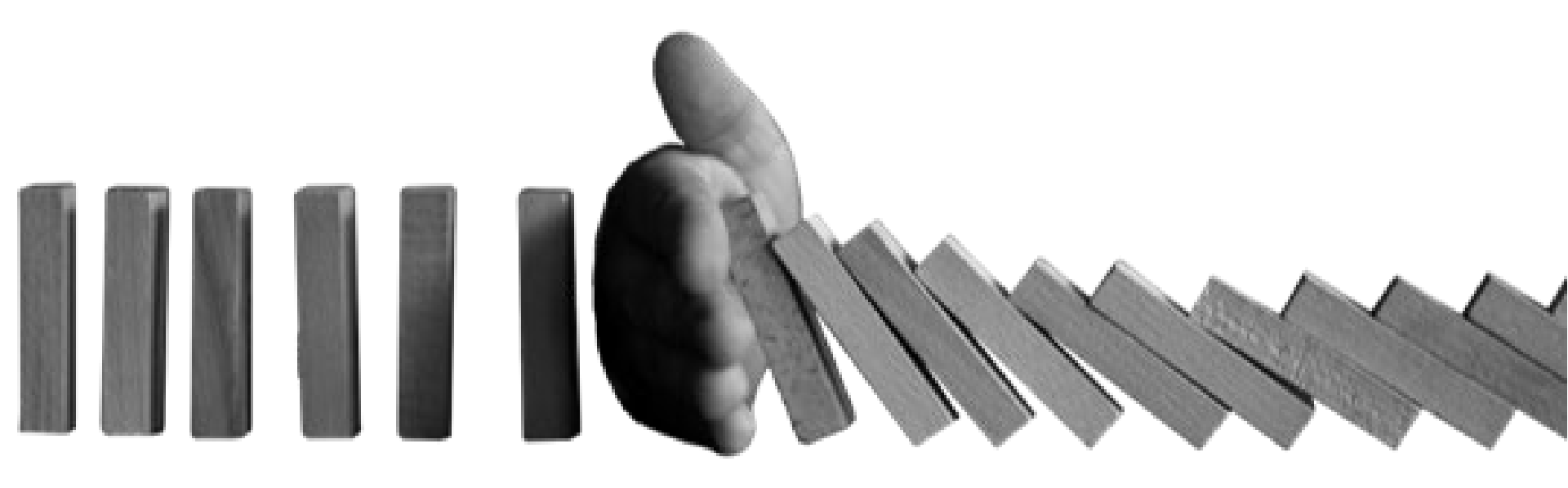
More than one in four receivers of breach ripple effects ended up paying all the costs



Ripples Across the Risk Surface, Cyentia/RiskRecon

I not only put myself at risk, I put an ecosystem at risk. I risk becoming Patient Zero in an attack on my sources, on my employer, my partners, on an entire supply chain.

Nicole Perlroth, former New York Times journalist and author of *This Is How They Tell Me The World Ends*



Shared risk requires shared defenses

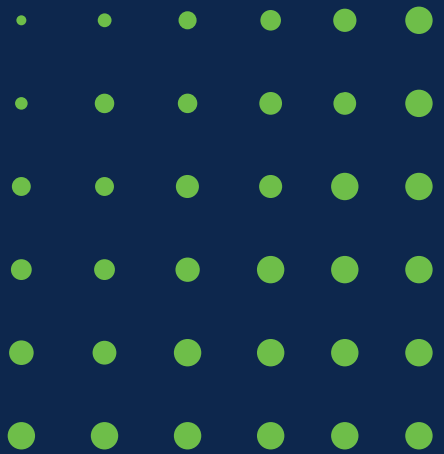
The notion of a shared defense is a statement of reality, not choice.

— U.S. National Cyber Director Chris Inglis

A durable solution must involve moving away from the tendency to charge isolated individuals, small businesses, and local governments with shouldering absurd levels of risk. Those more capable of carrying the load—such as governments and large firms—must take on some of the burden, and collective, collaborative defense needs to replace atomized and divided efforts. Until then, the problem will always look like someone else's to solve.

— Chris Inglis and Harry Krejsa, "The Cyber Social Contract"

The Security Poverty Line



The line below which an organization cannot effectively protect itself

What they need

- Money
- Expertise
- Capability
- Influence

Money

- **Can they actually afford the financial cost of tools and people?**

Expertise

- Do they know what constitutes essential security and how to go about implementing it?

I’m a new CISO. It’s my first day on the job in an organization that has never done security before.

What should I buy?

The Real Cost of Security 451 Research, 2013

Even the Experts Don’t Know

As few as 4 different technologies and as many as 31

Everyone said “it depends,” including the vendors

The minimum baselines pretty much matched up to PCI, and included both firewalls and AV

Budget could be off by as much as a factor of 4

There's still no guarantee you won't get breached

Capability

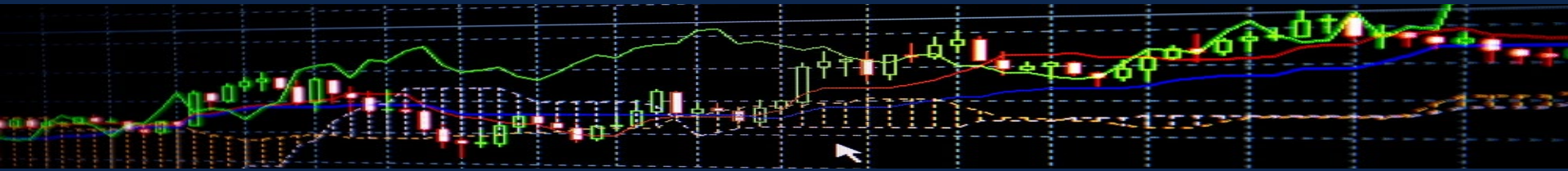
- Assuming they know what to do, can they carry it out, or are they blocked by situations or logistics?

Company Culture

Bleed to lead

Never disrupt the guest experience

We sell security; we'd better be good at it ourselves



Two Big Dichotomies

Safety vs. Security
Privacy vs. Security

Influence

- **Can they cause the right changes in their suppliers and stakeholders?**

What they need

- Money
- Expertise
- Capability
- Influence

In 1989, two things happened within weeks of each other: the Berlin Wall fell, and Tim Berners-Lee created the World Wide Web. This started the vision of a global world where we would all come together.

But now it’s the Internet of many in the hands of a few. If we want to return to a democratic state, we need to get it back to societal common ground.

Sarah Kriesche, freelance journalist

Starting With Fundamentals

Addressing the money problem

Expertise, not “awareness”

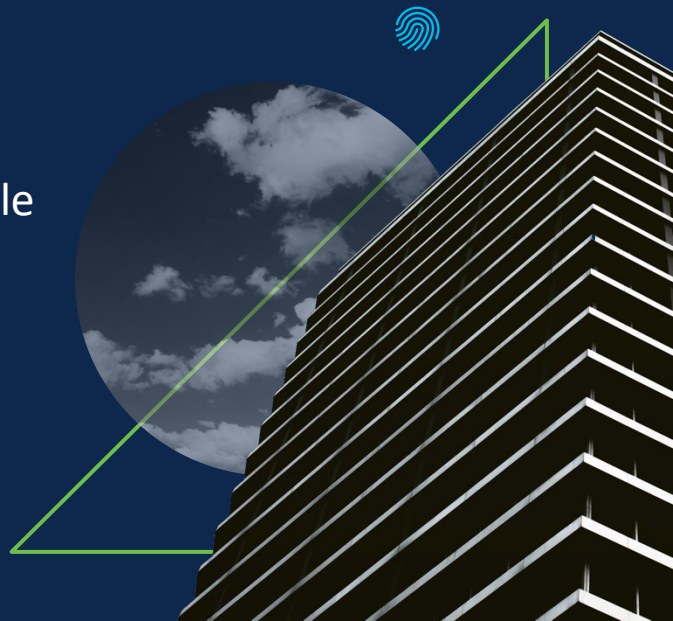
Capability: migrating from legacy environments

What we owe

- Money

Security costs and spending

- Is there a minimum amount that everyone should spend, or that governments should provide?
- Open source isn’t free if you need people to run it
- Should some basic security infrastructure or controls be provided as a subsidized service?
- What security should be “built in” and therefore available at no extra charge?

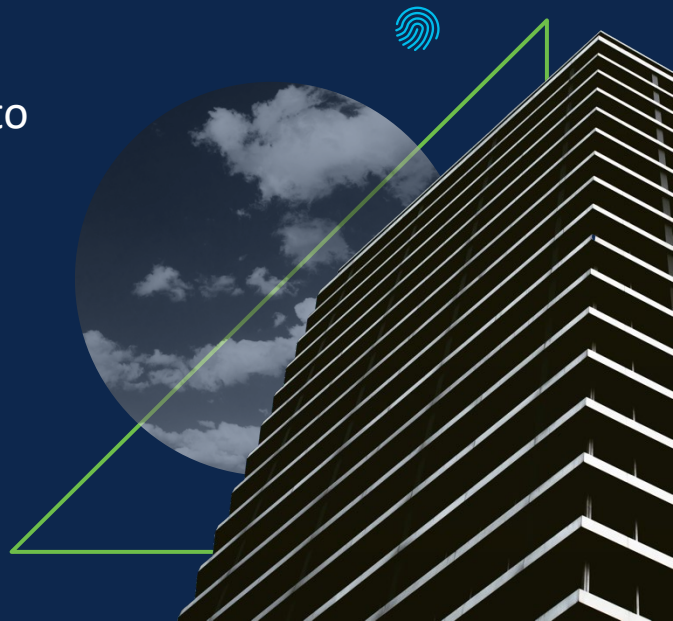


What we owe

- Money
- Expertise

Expertise: more than just “information sharing”

- Efforts such as the “NTSB for cyber” should help increase general knowledge
- Security products should be designed to require less arcane security expertise
- Visibility and transparency are necessary, but you have to know what to do with what you receive
- Support all entry paths into cybersecurity and push for retention efforts
- Stop the market-driven concentration of expertise in those vendors who can outbid for talent

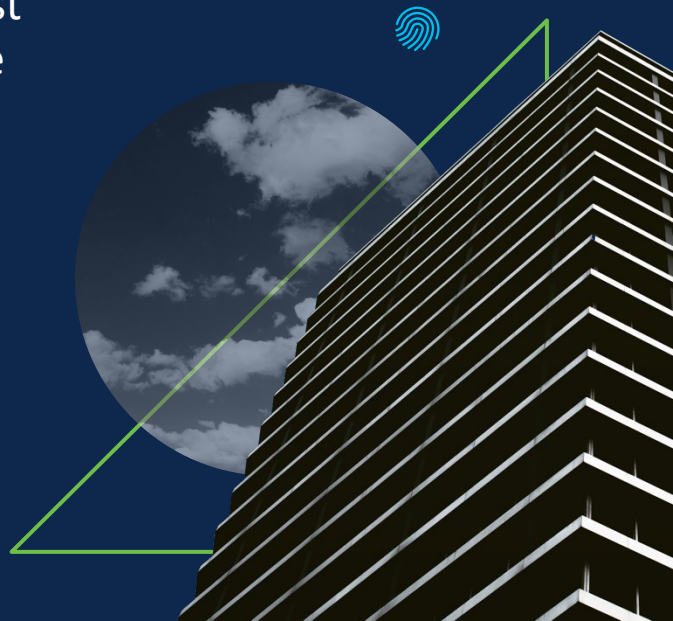


What we owe

- Money
- Expertise
- Capability

Architecture standards to help capabilities

- Enable better tech refresh and integration practices
- Move non-core business functions to cloud
- Vertical-specific security reference architectures (not just compliance checklists) to help with business and culture constraints
- Is there a shared responsibility model we can actually agree on?



Daniel Grzelak
@dagrz

What's that famous Tyson quote? Everyone has a shared responsibility model until they get punched in the logs?

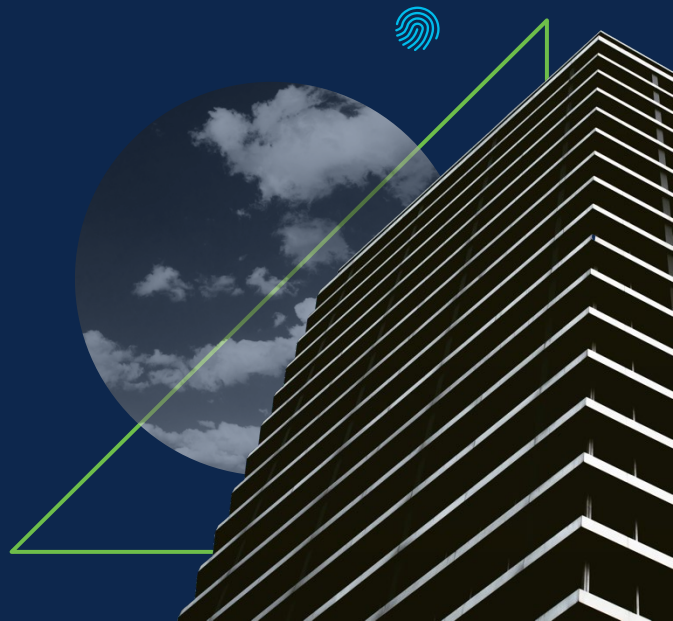
6:13 PM · Dec 11, 2021 · Twitter for iPhone

What we owe

- Money
- Expertise
- Capability
- Influence

Incentives and other collective influence

- Reduce risk externalities
- Identify “linchpin” components of the security ecosystem
- Balance risk-driven regulation between the biggest/loudest and the rest of the community
- Address the massive multi-stakeholder, cross-border, military/civil cybersecurity policy problem



I think we need to think about cyberspace as an environment, where we increasingly live and work. So that means we have obligations to each other. We have obligations to look after our bit of the digital environment. We've the obligation not to be digital pollutants. We've the obligation not to allow bad things to happen on our patch. We've the obligation to work in our personal and professional lives to help clean up the digital environment.

Ciaran Martin, CB

Professor of Practice in the Management of Public Organisations

Blavatnik School of Government

This may be as complicated as battling climate change

It is a pragmatic as well as a moral imperative


cisco
SECURE