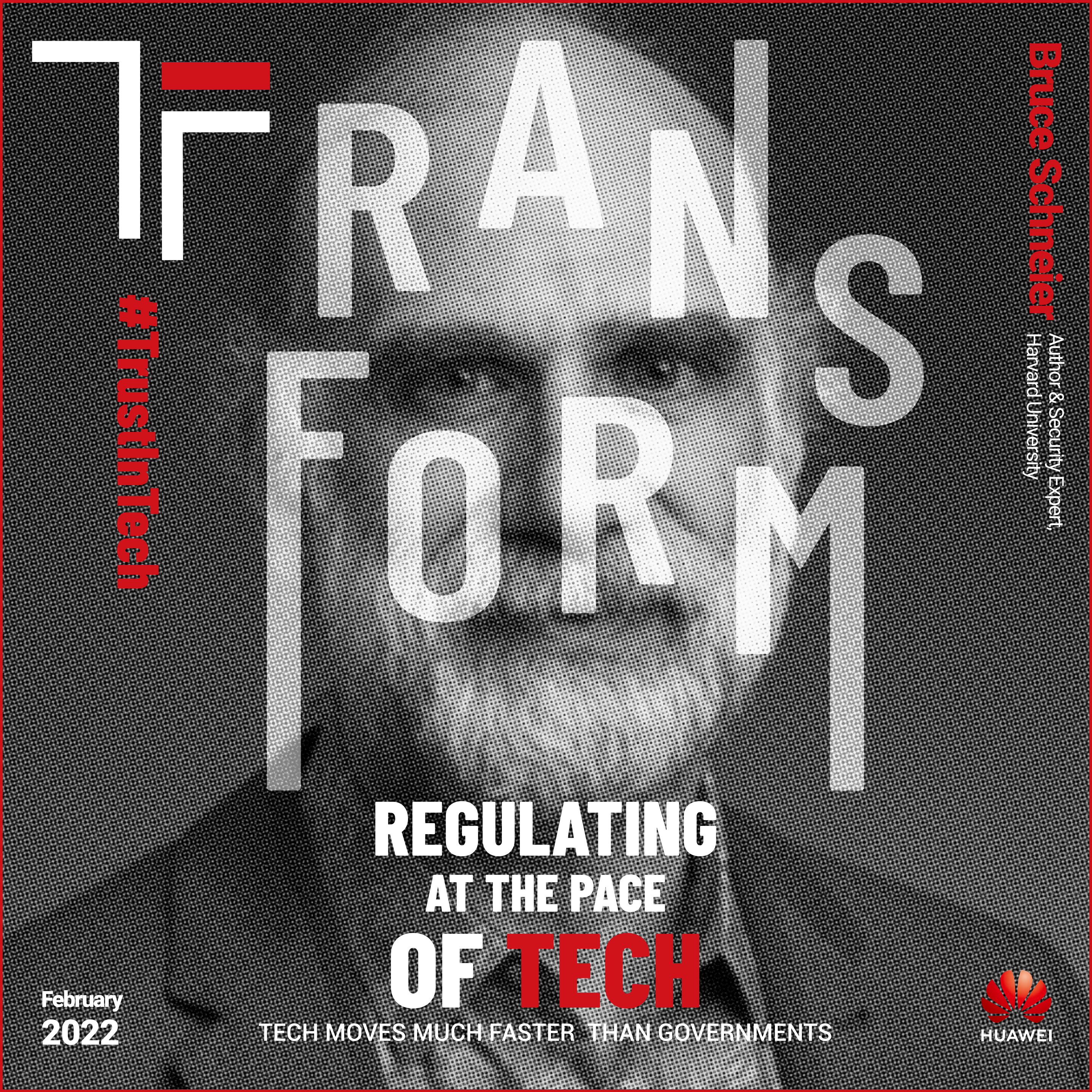


TRANSFORM

#TrustInTech

Bruce Schneier
Author & Security Expert,
Harvard University

REGULATING AT THE PACE OF TECH

TECH MOVES MUCH FASTER THAN GOVERNMENTS

February
2022

HUAWEI

IN THIS ISSUE,
WE LOOK AT THE SUBJECT OF TRUST IN TECH.

www.huawei.com/en/facts/transform

CONTENTS

EDITOR'S NOTE:

IT'S TIME TO CONFRONT THE ELEPHANT

Gavin Allen
Editor-in-Chief
Huawei Technologies

✉ Gavin.allen@huawei.com
@68tractorboy

Ignorance isn't bliss.

It's a thought that's occurred to me more than once whilst trying to navigate the complexities of tech. The risks and suspicions, the acronyms and ethics, the innovations and opportunities: it can all seem – to quote Churchill, as we Brits love to do – a riddle wrapped in a mystery inside an enigma.

And that feeling of bliss-less ignorance occurred to me again in a conversation with Bruce Schneier, a Harvard fellow, author and noted security expert, for this debut edition of Transform.

"Technology companies are creating the world," Bruce told me. "And letting them create the world for the short-term benefit of a bunch of tech billionaires is kind of a dumb way to run society."

When it's put like that, you can perhaps see why trust in tech – and its "bunch of billionaires" – appears to be on the decline in a number of countries.

> How can we trust tech giants? Few of us know what they're doing.

Even if we know, we often don't really comprehend what it means. And almost no-one, the giants included, can know where it will all ultimately lead.

So no, ignorance really isn't bliss. Which is one of the core reasons Huawei decided to start Transform – a publication aimed at providing insight into the present, plus a glimpse of the future. From the Internet of Things and blockchain to digital power and cyber security, our world is transforming around us, and it's in all our interests to be more aware of what those changes mean.

My entirely non-expert view is that the change will doubtless be bumpy in parts but ultimately exciting and transformative in a way that makes our lives easier and more connected. But then working as I do for a tech giant, perhaps I would say that, wouldn't I? Which is why the more open debate we can have about these current and looming changes – and the more light we can shine upon them – then surely the better.

Each edition of Transform will look at a single theme impacting the tech industry and therefore, in time, impacting you. And it'll do so in an accessible and (we hope) engaging manner.

The theme of the first edition is Trust in Tech, since trust surely underpins and eclipses every other consideration for consumers and innovators alike. And yes, it would feel a bit like skirting around a sizeable elephant in the room if Huawei chose to ignore the issue of trust.

In our headline discussion, the self-declared optimist Bruce Schneier explains why declining public trust scores in tech are actually a good thing – after a "collective indifference" we've woken up, he says, to the power of the industry.

But we need regulation and government help to hold tech to account and achieve the security and privacy we value.

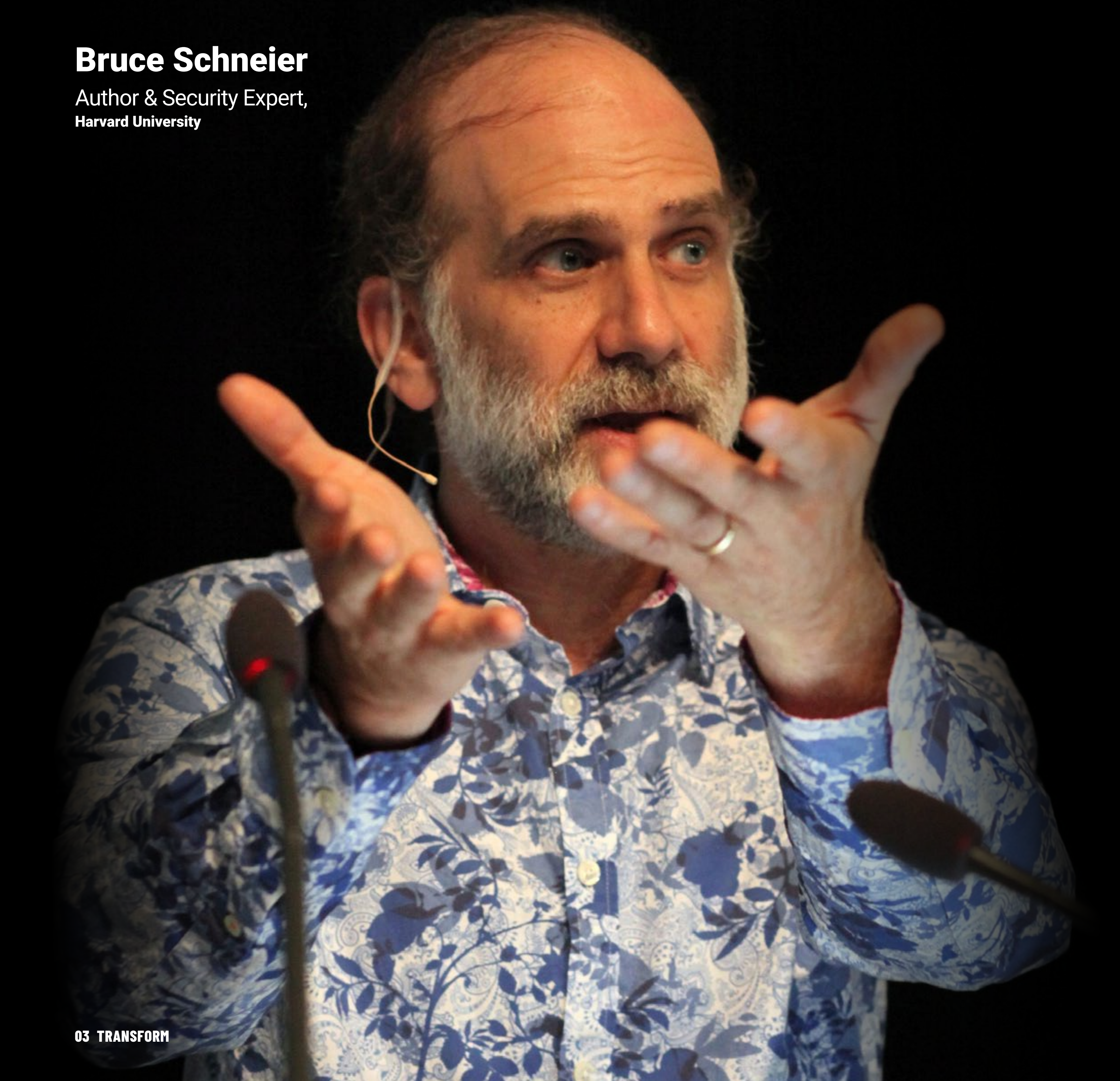
Bruce's main worry is that regulation is continually outpaced.

"What we have now is the level of computer security that the market rewards: not very good," he tells me. "The only solution is for tech to solve tech problems… The question is: does the market reward the problem-solving tech, or just the problem-causing tech?"

Elsewhere, the former Director-General of the World Trade Organization, Pascal Lamy, says we "need to mitigate de-globalization, in order to avoid making this world a worse place."

In addition, we offer a four-point guide to tackling ransomware, explain why fear of AI could give the bad guys a head start, explore the data trust rating system aiming to become the global standard, and still find space to guide you through the treacherous world of backdoors and network vulnerabilities.

And much more besides. We think Transform offers a rich list of interviews, essays, videos and thoughts: but I trust you to let us know either way…



Bruce Schneier
Author & Security Expert,
Harvard University

BRUCE SCHNEIER ON REGULATING AT THE PACE OF TECH

CYBER SECURITY EXPERT BRUCE SCHNEIER TALKS ABOUT REGULATION, MARKET FAILURE, AND WHAT KEEPS HIM UP AT NIGHT

Scan QR code
to watch the full interview video

Interviewed

by Gavin Allen

Gavin Allen: Bruce, thanks for being with us. "Can I start with public trust in tech, which we're told is falling?" It's a techlash. It's a crisis for tech. But actually, shouldn't we be saying it's a good thing? This is a kind of wake-up call that we're finally aware of the security issues around tech.

Bruce Schneier: I think people are saying it's a good thing. Over the past decades, we've kind of given tech companies free rein to do basically whatever they wanted. The technology was new, and it was "niche-y." Companies were building tools for techies, they were building tech tools, they were building toys. And sort of very rapidly, they became central to our economies, our societies, our friends, our families, the way we work and live - our democracies. And they became important. And now, this sort of ability that tech has to create the world as they see fit, is now seen a problem, a liability. It's definitely a wake-up call, it's a good thing. It shows the maturity of the tech industry. That they're now not these niche players you can ignore. That they're important. And it's a way to make tech truly part of our society, part of our fabric of life.

Gavin Allen: Do you think that when we, as the public, and I say the word "we" advisedly because me as well, when we point the finger perhaps at the sort of lax security, are we being slightly hypocritical? We're pretty carefree with the number of passwords we repeatedly use. We don't really update when we're told to on security issues. And isn't the problem that our expectation of full on, perfect cyber security will always fail, because people are in the system?

Bruce Schneier: You know, but you could say that about anything, right? What do we care about aircraft safety? Isn't it our fault for not being mechanics and not checking the aircraft ourselves, for not getting flight training? Are we pointing the finger at the companies mistakenly? Of course not. We're not experts in airplane safety or in computer safety and security, and we shouldn't be expected to. We expect the things in our lives to be safe. We walk into a restaurant and don't have to check the kitchen ourselves. We're not being hypocritical. We're recognizing that governments perform a valuable function in our stead: they are our experts. And yes, we hold airlines and restaurants and Internet companies to higher standards than we might have ourselves. And that's okay. That's proper. That's just the world.

Gavin Allen: It's also quite a relief to me, as I say, as a multiple same password user. So thank you for that. I got a free pass.

Bruce Schneier: Not to be unfair, you really should use unique passwords for important accounts. But it shouldn't be that your personal security failings should be catastrophic. We want you to keep food in a refrigerator, and not drink spoiled milk. But that doesn't mean that the manufacturers of these products don't also have to follow hygiene standards. So we kind of both do. What we're gonna hold the dairies to, and you, are gonna be different standards. We're not gonna hold you all to the same standards, because it's not that you don't know better, it's that you're not an expert in these things. And we want you as a non-expert to be able to use food that doesn't spoil, get on airplanes, go to websites, do all of those things.

Gavin Allen: Well, that's interesting on the topic of experts. Huawei has a zero-trust approach to cyber security and the sort of ABC of assume nothing, believe nobody, check everything. But that isn't really the industry standard, let's be honest, it is not observed across the whole of the tech industry. How do we incentivize...

Bruce Schneier: But it's not observed by Huawei either, right? I mean it's a nice idea, but it's never observed by anybody. I mean, you didn't verify my ID before you interviewed me. You don't know this is me, so you don't do it. You know, we're using a commercial piece of software for this interview. You haven't checked the source code. We typed a random password into a screen. What happened? We don't know. So zero-trust networks is a way of thinking about networks where you're continually authenticating. A lot of companies do it, but don't think of it as absolutely zero trust. That's as ridiculous as the perfect security idea you started with. But it's a way of saying, the old way was, you type in your password and now you're in and you can do anything. In a zero-trust network, we're continually checking to make sure you don't do anything bad. So an example might be, you can log into your bank account, but if you suddenly transfer your entire life savings to some dodgy account in Eastern Europe, the bank's gonna ask for some little additional authentication checks. That feels like a good idea. Right? It's not zero trust. Think of it more as variable trust. And yeah, it's done by some, not by others, but there's a lot of degrees here. It's not black or white or all or nothing. The name of zero trust makes you think black or white or all or nothing.

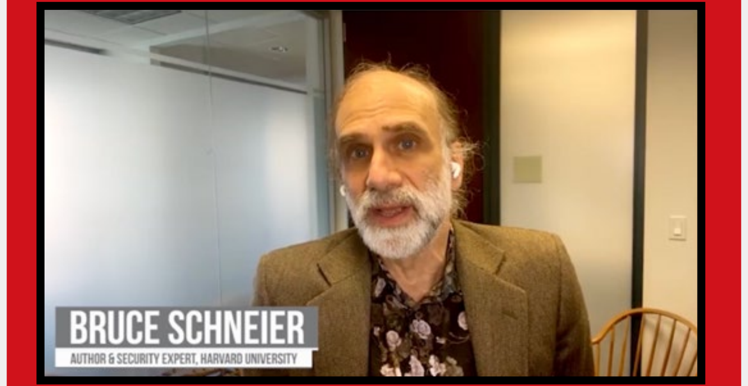
Gavin Allen: Well I think it makes you think of a mindset and an approach. It is more of a process, isn't it, than a sort of an actual fact in a moment, in time? But nevertheless, how do you get the market, I suppose, to reward safety and security and indeed that mindset?

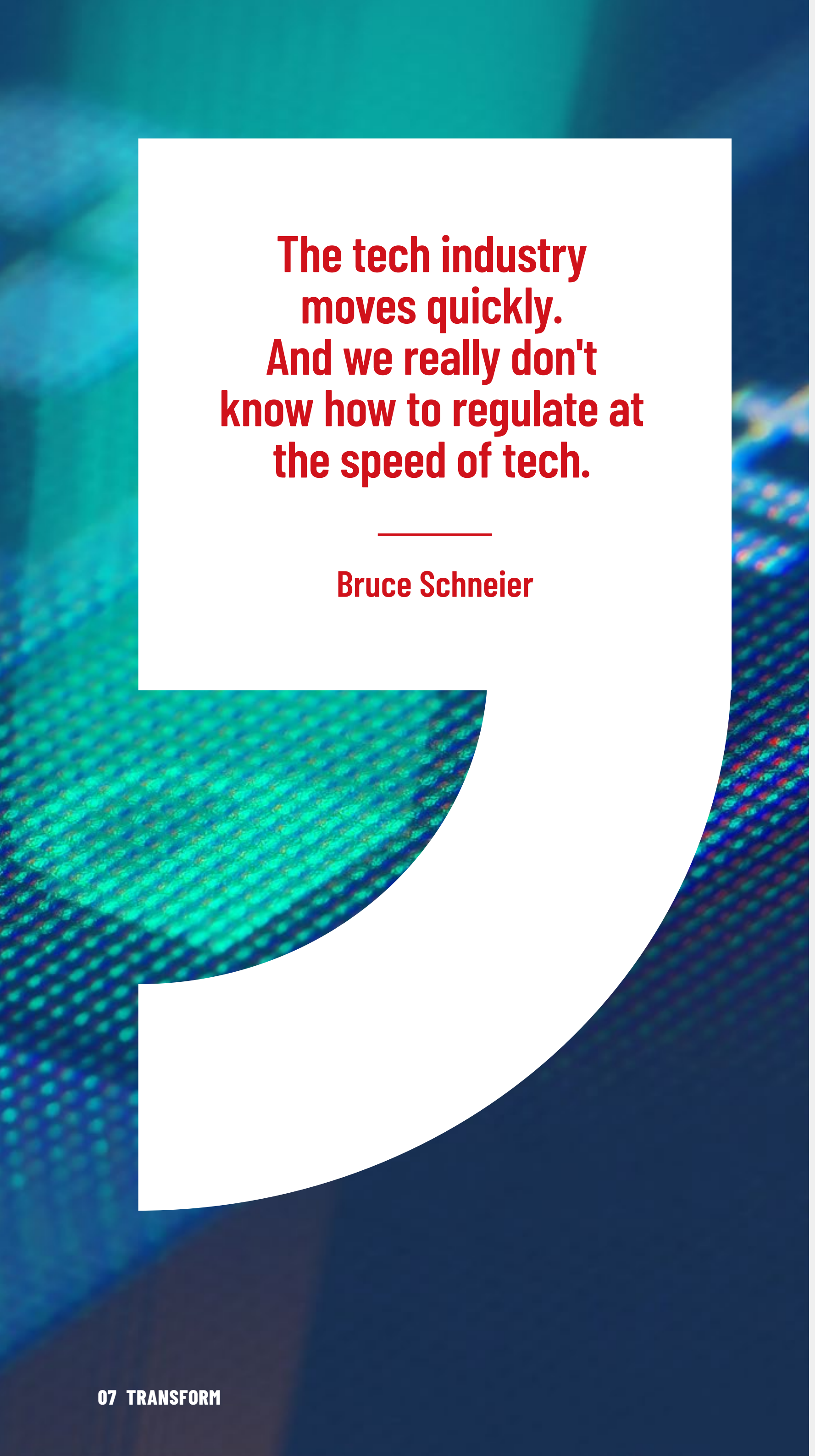
Bruce Schneier: This actually isn't hard. You regulate it.

How do you get the market to reward aircraft that don't crash, or pharmaceuticals that won't kill you, or pajamas that won't catch on fire? Or baby food that's actually nutritious?

You pass regulations. The market in every industry pretty much never rewards safety and security unless forced to by government.

What we have now is the level of computer security that the market rewards: not very good. If we want better, government has to mandate it. Government is the trusted entity that we turn to. Because I don't know about automobiles, and how they should be manufactured. I don't know about aircraft. I don't know much about, you know, packaged food goods - or pharmaceuticals. But I can go to a drugstore and know that everything on the shelf is safe. There's a lot of caveats here. But basically snake oil is not allowed to be sold in stores, and government is who makes that happen. It is not the market.





The tech industry moves quickly. And we really don't know how to regulate at the speed of tech.

Bruce Schneier

Gavin Allen: But you've called, in a lot of your essays and in your blogs, I've seen across a range of topics and certainly over a range of years, you've called for greater interventionism into the tech industry, greater regulation of it. Why do you think we are sort of still, presumably, in your view, still slightly off the pace on that? Why are we always playing catch up, or is that, again, is that an inevitability?

Bruce Schneier: Yes and no. I mean, talk about the United States, the United States just doesn't regulate. We, right now - you know, we're talking about trust, there's very low trust in government. The US government does not regulate industry in any meaningful sense. And despite all the rhetoric, all the hearings, all the strong words, we're not seeing meaningful regulation of technology in the United States. Or really in the UK. I mean right now, the EU is the regulatory superpower on the planet. If you want to see tech regulation, look at what the EU is doing. It's not great, but it's a start, and they are continuing. So I think the problem is sort of bigger than tech. The United States has a lot of trouble with governance in general. But also there's something that you said that the tech industry moves quickly. And we really don't know how to regulate at the speed of tech. Tech moves much faster than government, and we don't really have a good theory of agile regulation. The best we have, at least in the United States, are regulatory agencies, which are able to move faster than congress can, but still slower than technology. So I think right now we in society, we're working out how to regulate technology at technology's pace. You know or, we pass regulations on Facebook today and by the time they get enforced, Facebook is well beyond it. They're Meta and they're different, just like when the United States tried to regulate Microsoft and Internet Explorer. By the time they did something, it was too late.

Gavin Allen: And again, that's that sort of catch up element, but also you touched on something there about the EU leading the way, America having its own specific issues. Can you have proper regulation, and interpret that in whatever way you want to, but proper regulation of a global industry in such an interconnected global industry without a global series of treaties?

Bruce Schneier: Don't know. It's an interesting open question. I mean we do regulate international things. Right? International airplane flights, shipping. Pretty much all of our supply chain is international. So there is a lot of international regulation. What you're getting at, I think, more precisely said is, what's the proper regulatory footprint that matches Facebook, which has more users than Christianity, and is larger than most countries? We don't really have the right regulatory body to deal with the Facebooks and the Googles and the Apples and the Microsofts and the Amazons. So there's this mismatch between regulation size, which tends to be countrywide, and these companies which are global. Now, do we need international regulatory bodies? Yes, but they move really slow. If you think about you know international shipping regulations or telephony, the ITU which regulates telephones. I mean these are ancient, stodgy, moribund, regulatory agencies, not suitable for the Internet. So we need to figure this out as well.

Gavin Allen: I was interested in a quote that I read in The Economist recently, which talked about counterproductive, knee-jerk, techno-nationalism, which again is maybe a sort of flip side of what you're saying about, the sort of individual areas having individual views on the world. Do you think that will hinder the development of cyber security or actually help the development of cyber security, if there is this techno-nationalism?

Bruce Schneier: Some of each. Some of the techno-nationalism is okay. Germany, France, United States, Japan, have very different laws about free speech. And why is it that the United States, which is an outlier in the way we have free speech laws, is exporting our law to these other countries? Does that make any sense? Germany and France have laws about Nazi memorabilia, whether you can sell it or not. It's legal in some countries, not in others. There are different standards on pornography. And there are countries that you know deliberately censor speech. So there are differences in the way countries work in their laws, and it seems reasonable the internet should respect them. Usually it's the companies that complain we can't possibly do this. So you know therefore, we're gonna flout the laws in a bunch of countries. I don't have a lot of sympathy for that. So while some harmonization, I think, is valuable, countries do get to make their own laws. And by and large, I think companies need to respect that. It's when things get exported that shouldn't. So if one country has stronger censorship laws, does that mean what they censor is censored everywhere? Right now, what's the responsibility of these companies to push back against censorship laws, to push back against anti-democracy? And now it gets very complicated, because Facebook is the biggest censor on the planet. They censor more things than any government does. Who gave them that authority? They're not doing it for anybody, but them, they're doing it for profit motive. That feels even worse. So there's a lot of complicated things here to tease apart.

Gavin Allen: That's true. Facebook is interesting. And is there a danger though, that sometimes there's not the will to regulate in the full way? Because actually being able to point the finger at Facebook and other companies, it's not unhelpful to some politicians, because as you say, this is a complex problem.

Bruce Schneier: And I'm from the United States, where we have no will to regulate anything. So yes, that's definitely a problem. These are American companies.

Gavin Allen: Just going back to something you said about agencies and there's myriad agencies in America or across the world. Something I was interested in that you wrote on your blog in the last few years about offense and defense, to use American terms, which was about the way that agencies...

Bruce Schneier: What do you use instead of offense and defense?

Gavin Allen: Well attack and defence, but there you go.

Bruce Schneier: OK, I guess that's close enough. All right. I was curious. I didn't realize that was Americanism.

Gavin Allen: It will be an international language. Don't worry. But how do we encourage agencies when they spot vulnerabilities to fix those vulnerabilities, which is the defense, as it were, rather than go on the offense by spotting the vulnerability, leaving it open, and using it as quite a handy conduit to monitor rivals, should we say?

Bruce Schneier: You know, it's the same as all of the answers. You make one of these things illegal. How do you incent people to do one thing and not the other? You pass laws. Right? That's how we incent people not to burglarize each other's homes. This isn't hard. The behavior we want, we need to make cheaper than the behavior we don't want. So if you can be fined, if you can be sued, you're less likely to do the thing that is bad for society. And this again, gets back to government will to regulate.

Gavin Allen: Great, but I saw a quote from Elon Musk, I'm sure you're familiar with it, from 2014. Where he said we have to be...

Bruce Schneier: Never heard of him.

Gavin Allen: I knew you'd take this well. He said we have to be"**super careful with AI, potentially more dangerous than nukes." And that "lack of AI oversight is insane."** And again, this goes to your regulation point, I'm sure. But do you think his warnings, your warnings actually, in fairness, I'm sure over the years, do you think they have been heeded? Or is there still a kind of collective insanity when it comes to oversight of AI?

Bruce Schneier: Less collective insanity and more collective indifference. I think that most people are content to let private corporations do what they see fit. I don't have the same alarm over AI that Elon Musk and some others have. I think they had a continuum of technologies. And I worry about the technologies of today. I mean it's not like AI driverless cars I worry about. It's computer connected and assisted cars with drivers that I'm worried about. So a lot of the risks that people see in AI, you see today. And others are these far future science-fiction risks you only see in the movies. So there's a mix of both here. But

I do think we need to recognize that technology companies are creating the world. And that letting them create the world for the short-term benefit of a bunch of tech billionaires, is kind of a dumb way to run society.

And I don't think we should do it.

Gavin Allen: Yeah, you said recently, and it was this year, it's easy to let technology lead us into the future. We're much better off if we as a society decide what technology's role in our future should be. I won't ask you what do you think that future should be, because that might take quite a long time. But again, why haven't we done that? What is it about society that says, we'll let the tech guys do it? They're all terribly clever that you know you go and do your thing.

Bruce Schneier: Because that's what we do. We, especially in the United States, are a rights-based society, where you can do anything unless it's prohibited. The EU is more of a permission-based society, where you need permission to do something new. But even there, companies generally have the right to do what they want. And that's largely been okay up to now. It really is only the recent decades, where things like cyber security, or climate change – sort of these massive global problems – where you can't let companies do what's in their short-term self-interest and assume it will be in the long-term best interests of society. Whereas even 50 years ago, for the most part you could.

There was a saying in the United States, "What's good for GM is good for America." It's very Fifties: what's good for that big car company is good for all of us. And I don't know if it was true back then – I'm not a student of history – but it's definitely not true today.

Gavin Allen: Yeah, I think that does absolutely play into that issue of trust and trustworthiness and earning people's trust and actually our changing perception of that. I must quote you again because it's important you have more quotes than Elon Musk in this.

"Even though criminals benefit from strong encryption, we're all much more secure when we all have strong encryption."

Do you think it is still encryption, as you said in your book, Click Here, do you think it is still the single, most essential security feature for the Internet?

Bruce Schneier: I don't know if I ever said it was a single most essential security feature. Encryption is a tool. It's a tool for privacy. It's a tool for confidentiality. So when the tool is useful, it is a very important tool. When you don't need the tool, it's not very important at all. But especially as computers permeate our lives – like, move away from the screens, the laptops, the phones, into our cars, our appliances, and infrastructure – that keeping them secure is vitally important. As long as there is a cell phone in the pocket of every legislator and CEO and police officer and judge and election official, it's vitally important that they be secure. And encryption is one of the technologies of security, it's a very important technology. And securing those things, because they're so essential to our infrastructure, is far more important than having back doors so that law enforcement can investigate crime. We are safer and more secure because of that.

Gavin Allen: Yes, exactly. Now, in terms of that safety and security, I think again you said that the more complex a system becomes, perhaps inevitably the more vulnerable it is to hacking. And it feels to lots of us that the world is ever more complex digitally, as we perceive. Does that mean, again inevitably, we'll be more vulnerable to hacking, we'll be more vulnerable, full stop, less secure, and just the system will be less trustworthy?

Bruce Schneier: Inevitable is a tough word, right? Because that's for all time. Right now, what you're saying is correct. Complexity is the worst enemy of security.

As systems get more complex, they get less secure. The Internet is the most complex machine mankind has ever built, by a lot. Computers are incredibly complex. So yes, complexity is adding insecurity. Our security is getting better, but we are kind of losing ground because of that complexity.

That is not a natural law. That is a balance right now between attack and defense. Those balances do change. If you think about the history of warfare, you can point to a dozen or so changes over the centuries between attack and defense. So it's not inevitable, but it is true today. So, it is more difficult to defend than to attack. Doesn't mean it's futile, doesn't mean we don't try, doesn't mean we don't get better; but it means we're starting out at a disadvantage.

Gavin Allen: Do you think one of the – maybe the savior for us or at least the savior of tech could be tech? In terms of the ability of AI to root out and tackle the issues that really concern us, whether it's deep fake or whatever it might be. There's a greater incentive, a greater market demand, so tech comes full circle.

Bruce Schneier: We're surely not going to de-tech our way out of this. Right? We're not gonna go back in time and give up all our technology. So the only solution is tech to solve tech problems. And there's a lot of work in this. This is not a new idea. The question is, does the market reward the problem-solving tech or just the problem-causing tech? And there again, regulation is how we as citizens affect our lives, as opposed to we as consumers. Or a better way of saying it is how we act collectively as citizens instead of individually as consumers.

Gavin Allen: And are we getting that balance right? Because obviously, if we can have...

Bruce Schneier: No, I'm not getting it right. Are you getting it right?

Gavin Allen: Not personally, I'm sure, as you observe the security...

Bruce Schneier: Clearly this is hard and it's an ongoing process.

Gavin Allen: But you think that the importance of getting the balance in terms of the regulation, but protecting our values, our freedoms, our privacy, our liberties, basically. Do you think are we getting... Are we sort of, at least on the right side of that, and better to be erring towards the freedoms than the regulations?

Bruce Schneier: I don't know. I think we err towards corporate profits right now. We'll see. I am optimistic. I might be sounding pretty pessimistic, but I actually think humanity will solve this problem. And this is not the end of the great democratic experiment. This is, we will figure this out, we've had bigger crises in our history. And this isn't going to be the last one. But right now, it looks pretty difficult.

Gavin Allen: I'll pick you back up on the optimism, because it's the final question I was going to ask you actually. Looking ahead, what aspects of technology are you optimistic about? And conversely, inevitably, what keeps you up at night?

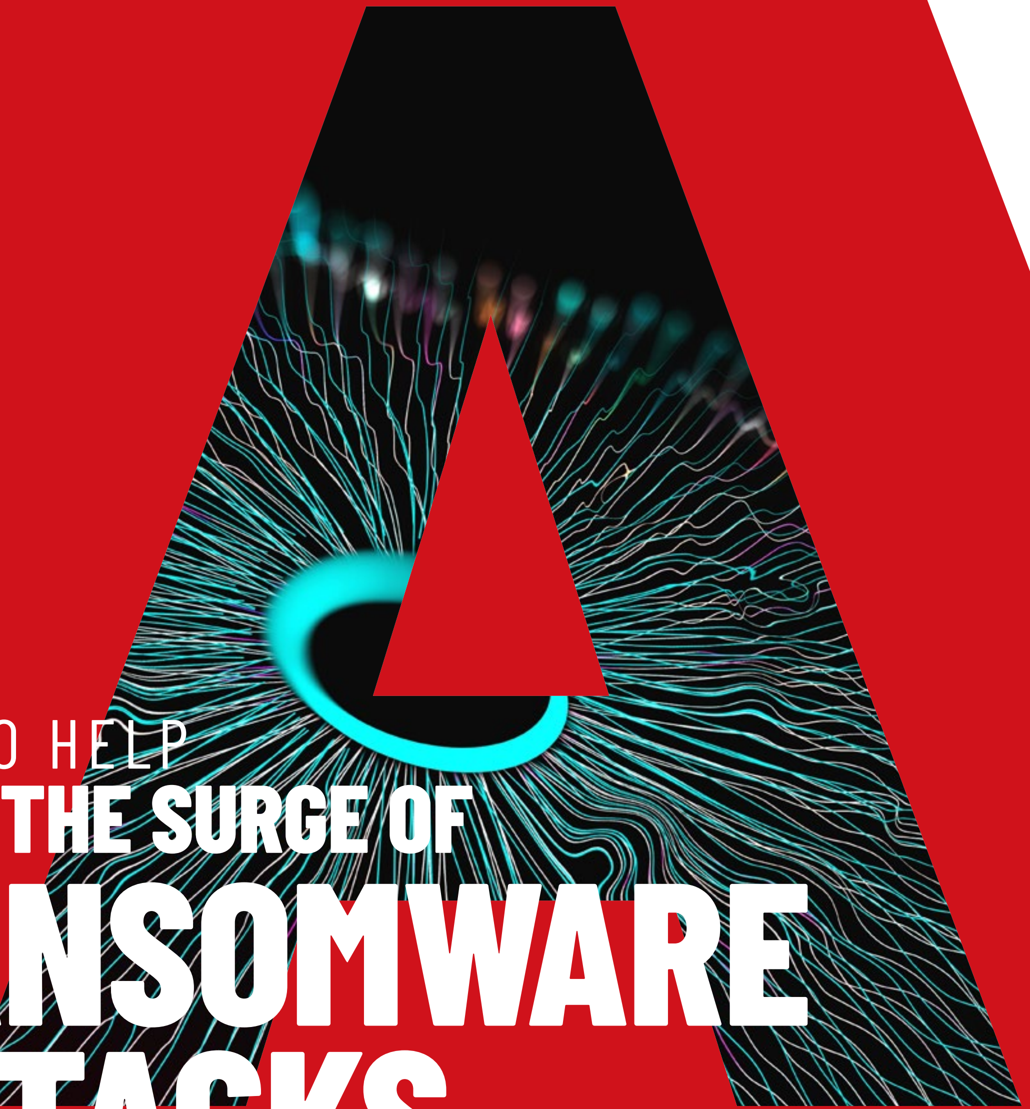
Bruce Schneier: I tend to be optimistic about the whole thing. It's not a particular aspect of it. It's that we as people, as humans, as society, solve problems. It often takes us a couple of generations – it might even take us a war – but we do. And society improves, century on century. And I don't think this is going to be the century that disproves that rule. I think it's all gonna be complicated. There's a lot of forces going on. Income inequality is an enormous force we haven't talked about. But it's one of the reasons why the United States, as a lawmaking institution, is failing. We tend not to pass laws that the rich don't like. And that's hard. But I think we will figure this out. What keeps me up are all the short-term issues. We need the short-term problems not to overtake the long-term solutions. And right now that's an open question. I'm optimistic, but I'm not at all sure.

Gavin Allen: Well, that's not a bad place to finish: optimistic, but not at all sure. That's great. Thank you very much Bruce for joining us. I really appreciate it.

Bruce Schneier: Thanks for having me. This was fun.

”

We're surely not going to de-tech our way out of this. Right? We're not gonna go back in time and give up all our technology. So the only solution is tech to solve tech problems.



HOW TO HELP STOP THE SURGE OF RANSOMWARE ATTACKS

by **Andy Purdy**

Andy Purdy
Chief Security Officer
Huawei U.S.A.

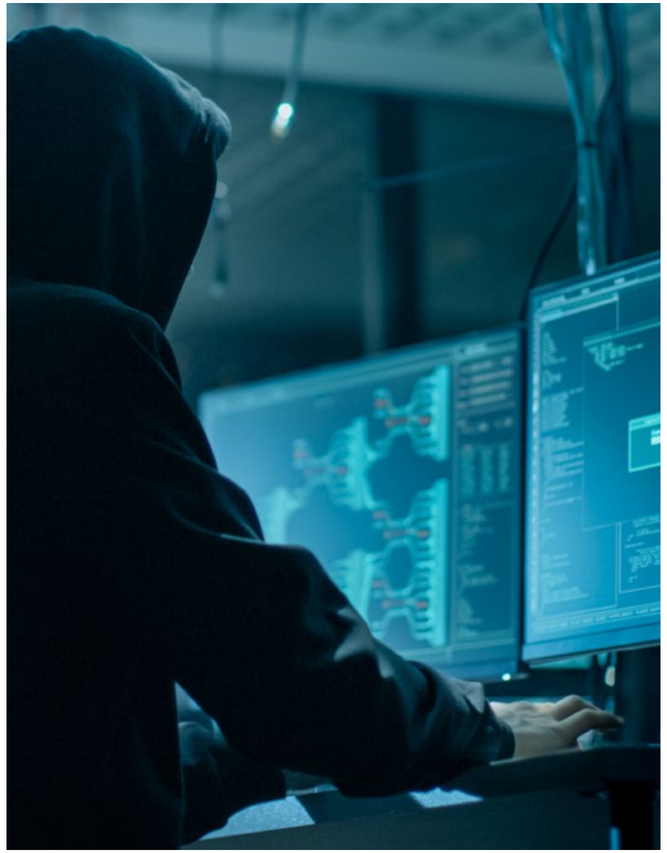
Call it the Year of Ransomware. Global attacks increased by 151% in the first half of 2021, surpassing the total volume for all of 2020. Victims included a major U.S. oil and gas pipeline, Ireland's national health service, and the public school systems in Maryland and New York state. French insurer AXA was hit just days after announcing it would no longer cover damage for ransomware attacks in its home market.

These attacks inflict real damage. One survey estimates the average total cost of recovery – including downtime, labor, and ransom – at more than $1.8 million per attack.

Even that number seems low. The Illinois Attorney General's office, hit in April, chose not to pay the ransom but spent $2.5 million to repair its computer systems and communicate with people affected by the breach. State lawmakers subsequently increased the AG's cyber security budget by $8 million.

Many companies see paying ransom as the quickest way to get their businesses up and running again. But the FBI says it just encourages more attacks, and experts are debating whether payments should actually be outlawed in order to remove the economic incentive. AT&T's former Senior Vice President and Chief Security Officer advises victims with no other options to "pay the damn fee" – then take steps to make sure it doesn't happen again.

What can be done about ransomware?



First, vulnerable companies – which is almost all of them – should be incentivized to increase their cyber security preparedness and held accountable if they fail to do so adequately. The Biden Administration is exploring "how to accelerate voluntary adoption" of improved cybersecurity measures. Still, only federal agencies and government contractors are currently required to follow certain cybersecurity guidelines.

Organizations that operate without adequate protections in place should face consequences to a much greater extent than they do now. We need the ability to assess the effectiveness of risk management controls before there is a breach or attack. Moreover, companies must be held accountable if they fail to meet stipulated requirements, even if a breach hasn't occurred yet. As businesses collect more data, they must proportionately increase their investment in cyber risk management.

Far too many companies, including a fair number of the Fortune 500, lack adequate cyber defenses.

Ignorance is no longer an excuse: the Cybersecurity and Infrastructure Security Agency (CISA) recently issued a fact sheet outlining how companies should protect themselves against ransomware attacks. A world of resources is at companies' fingertips.

Next, the private and public sectors should share information about cyber threats, vulnerabilities, attacks, and attempted intrusions. As I wrote in my last post, the White House recently issued an Executive Order (EO) to help strengthen the cyber defenses protecting government agencies and critical infrastructure. Among other things, the EO requires companies contracting with the government to disclose any significant cyberattacks.

While this requirement is a good first step, every company – not just government contractors – should be working with governments and other organizations to share information on cyber incidents. Faster, more complete sharing of information will improve our collective ability to anticipate and respond to cyberattacks. And this cooperation should extend to relationships with governments overseas and global companies. As things stand, the bad guys simply have too much of an informational advantage over the defenders.

Then there's the SBOM, or software bill of materials. An SBOM lists the components in a software product much as a label lists the ingredients in a can of soup. If a piece of software turns out to have vulnerabilities, an SBOM makes it easier to track the components, locate the source of the problem, and implement patching or other risk mitigation measures. Serious consideration should be given to the idea (referenced in the EO) of incentivizing or requiring software suppliers to provide an SBOM.

Performance targets are another potentially helpful measure. In July, President Joe Biden signed a memorandum that directed government agencies to come up with performance goals for critical infrastructure. This "industrial control initiative" aims to develop and deploy systems that warn of an impending cyber threat to critical infrastructure. Already, 150 electric utilities serving 90 million U.S. residential customers have agreed to deploy technologies that will guard against such attacks.

President Biden's EO shows that his Administration is committed to unifying what is currently a patchwork of industry-specific statutes and regulations that makes it hard to tell if U.S. critical infrastructure is as secure as it needs to be. The attack against Colonial Pipeline might have been averted if better systems had been in place. Implementation of performance targets can make it more likely that they will be.

Finally, to help reduce malicious cyber activity, including the spread of ransomware, countries need to develop global cyber standards and best practices to govern the protection of data and the online conduct of both companies and sovereign states. We must also promote greater transparency, as well as conformance and testing protocols, while creating mechanisms that enable real accountability for nonconformance by governments and private organizations.

The EU's General Data Protection Regulation (GDPR) is an example of how compliance requirements can be adopted across many different countries, including several that are not a part of the EU. One big reason why GDPR has worked well thus far is that it provides very strong guidance for appropriate conduct and metes out serious penalties for violations: up to 20 million Euros or 4% of a corporation's revenue – whichever is greater.

Similar types of standards (or other rules of the road) and conformance protocols are needed to create momentum toward a safer and more transparent cyberspace. Mechanisms should be developed to try to hold private organizations and national governments legally accountable.

While these measures won't stop ransomware completely, they can help reduce their frequency by decreasing the economic incentives to perpetrate attacks and increasing the cost to cyber miscreants.

> **"Every company – not just government contractors – should be working with governments and other organizations to share information on cyber incidents.**

Mika Lauhde
Global Vice President,
Cyber Security and Privacy,
Huawei Technologies

FEAR OF AI COULD POSE THE BIGGEST CYBER RISK OF ALL

EXCESSIVE CAUTION COULD ALLOW THE BAD GUYS TO PULL AHEAD.

Quick, think of a scary technology – one with the potential to enslave humankind or destroy the earth.

Did you think of AI?

Few other technologies generate the fear factor of artificial intelligence. Ever since Alan Turing introduced the idea in 1948, people have wondered what would happen if machines outsmarted their creators and took charge of the planet.

Legal protections could avert such a calamity, and the first AI regulations have been published and are awaiting public comment. But some of these draft rules set impossibly high standards. For example, a proposed EU regulation on AI released this year requires that all data sets used for machine learning be "free from error."

Few data sets are. A recent MIT review of 10 major data sets found an average error rate of 3.4%, which translates into tens of thousands of errors, including mislabeled images, text, and audio.

Tech companies are already expressing concern about the EU regulations. Google was diplomatic, saying the company "is concerned that the opportunity cost of not using AI is not sufficiently reflected in policy debates."

It's understandable that legislators are cautious. But **excessive caution creates another risk: that while "bad guys" move full speed ahead to use AI for malign purposes, "good guys" proceed carefully,** waiting until every last lawmaker, skeptic, and late adopter is fully convinced that AI should be trusted rather than feared. If we take this two-track approach – bad actors moving quickly while good ones drag their feet – the results could be grim.

Hackers are already using AI to create botnets, guess passwords, break CAPTCHA systems, make illegal robocalls, and engage in other forms of cyber mischief. They don't care about collateral damage, and they don't need to think about certification, testing, or regulatory compliance. Unfortunately, this means that **right now, bad people are using AI in more advanced and innovative ways than good people are.**

That will likely cause some – perhaps many – to distrust AI even more than they do now.

But good actors outnumber bad ones, and over the long term, the odds are high that AI will be used in ways that benefit society. In the meantime, what can be done to build trust in AI?

The simple answer is that for now, we should not try to achieve full trust in AI. Instead, we need to build just enough trust that we avoid over-regulating AI in a way that lets the bad guys pull ahead. We can do that in several ways.

First, we must ensure that cyber security experts are familiar enough with AI to avoid unintended consequences. For example, in trying to use AI to solve a conventional security issue, one might inadvertently cause it to create a totally unforeseen, and undesirable, "solution."

Again, bad guys don't have this issue. In fact, they are probing for loopholes in cyber defenses against AI. For them, unintended consequences are a boon that could reveal hidden weakness to be exploited.

The need for AI-savvy cyber security people will compound an existing talent shortage: by some estimates, the world needs an estimated 3 million more cyber security professionals than it currently has. But in addition to conventional skills – knowledge of network architecture, access control, encryption, and so on – cyber security experts increasingly will need the ability to work with AI to create trustworthy solutions.

Second, we will need to create the right IT environments to defend against AI-led attacks. AI is often considered to be a general purpose technology – one with so many uses that it affects all aspects of society.

But AI will be less "general purpose" when operating within specific environments. For example, every corporate IT system is different. They have different password schemes, access controls, and firewalls; their users behave differently. This means that, in a badly structured or poorly operated IT environment, AI will learn bad habits. It will generate false positives and false negatives. People will eventually conclude that AI can't be trusted.

But in the right environment – one created using best practices, clear processes, good management and good tools – AI can be trained to spot anomalies and deviations from normal activity patterns that signal a security breach. AI will function like a well-trained guard dog that spots intruders and keeps them away. Once it begins behaving that way, people will start to trust it.

Third, we must work even harder to narrow the digital divide. Most people don't link the issue of digital inequity with cyber security, but the connection is real. AI can rapidly harness computers for botnets or attacks. In some developing countries, companies may lack the capabilities to create a better structured, more robustly protected IT environment. That makes these countries a rich hunting-ground for cyber criminals.

Just because a problem isn't in your network doesn't mean it's not your problem. Vulnerabilities can migrate – another reason to help poorer parts of the world start benefiting from more advanced technology.
The key to solving these issues is international cooperation. Like Covid and climate change, AI's security implications don't respect national borders.

To be sure, there are significant barriers to trust among nations at the moment. But if we cannot establish a degree of trust sufficient to collaborate in this vital area, we will inevitably start to view AI not as a trusted tool to be utilized, but as a threat to be feared. If that happens, the bad guys will have an insuperable advantage – not just for now, but forever.

> **We should not try to achieve full trust in AI. Instead, we need to build just enough trust that we avoid over-regulating**

TRUST IN TECH SUMMIT

DECEMBER 2 2021

REMARKS BY PASCAL LAMY, PRESIDENT OF THE PARIS PEACE FORUM. "BRIDGING GLOBAL GAPS"

Scan QR code
to watch the full video

Like most of my friends and colleagues participating in this year's Trust in Tech Summit, I have spent quite a bit of time since 20 months thinking, working, listening and discussing about how a post-COVID world would look like if and when there has to be one, which we all hope what I want to do today is to share with you my answer to this question, and how I believe trust in tech can help address the consequences of what I see now, unfortunately, as a more divided world than in the past decades.

The theme of the Paris Peace Forum, which just took place mid-November and which I have the privilege to chair, was "mind the gaps".

Global gaps in this world are getting wider, not just because of COVID. What is the role of tech in bridging these global gaps?

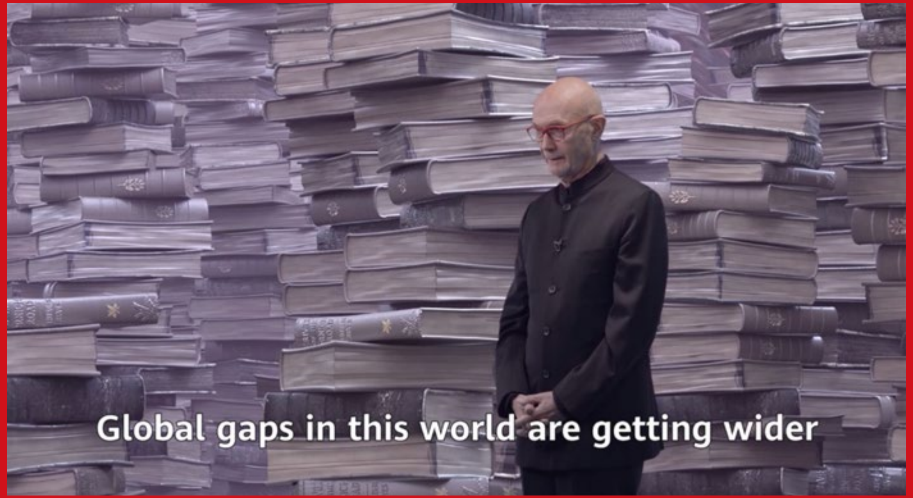
That global gaps are getting wider, is pretty clear if you look at the main global trends.

Let me take three examples: climate, digitalization, and geopolitics.

Starting with economics:

> **"The economic divide between north and south, between rich and emerging countries, on the one side and poorer ones on the other is increasing.**

For the first time in 50 years, the COVID crisis will have interrupted the slow long term convergence in growth rates between rich and poor countries on this planet. More poverty, more suffering hence more social and political tensions.



A new climate divide is also appearing, not just because of the disproportionate impact of global warming on some weak countries, but also because of the heterogeneity of mitigation and adaptation, national strategies and measures. Time horizons for zero net carbon are different, ranging from 2050 to 2070. For countries who have such a time horizon, carbon peaks take place at different periods. Policy tools such as taxation, emission trading system, regulation, various incentives are different and this will likely result in a more unlevelled playing field for international trade.

COVID has also accelerated the digitalization of our economic and social systems. Digital capacity gaps are widening among countries, as well as inside many of our populations, where skills and production systems will have to be profoundly reshaped, transformed with the likely ensuing turbulence.

As if this was not enough, geopolitics are adding their own toll on these worrying trends. Whatever the reason for this evolution, and both sides have their own interpretation about that, the US and China are now engaged in many areas in a more intense rivalry than in the past, thus raising the level of stress on the rest of the world. Decoupling or dual circulation are now becoming fashionable on both sides, with more search for self-reliance, at least in sectors of production of goods and services deemed critical for security or strategic reasons. The EU has also started to think in similar terms, although less aggressively.

All in all, some new kind of fragmentation is underway that will impact the economics of the rest of the world. If I look back through my nearly 40 years of engagement in international economics my sad feeling is that this world has recently changed course. From previous dynamics, when geo-economics who tend to integrate, superseded geopolitics who tend to divide, to a different balance where geopolitics now supersede geoeconomics. One in which the zero games of power games have become more than the positive sum games of cooperation.

When I had to pass my hearing at the European Parliament in 1999 to become EU trade commissioner, my vision was that we needed to harness globalization in order to make this world a better place. Today, some 20 years later, I would probably take a different stance. I would say that we need to mitigate de-globalization, in order to avoid making this world a worse place.

This is where tech and trust in tech comes in big way. I think that tech, with digital tech in the front line, can be a formidable tool to bridge these global gaps. But I also believe that this tool needs to be properly governed on a global scale to avoid further divisions.

That digital tech is key to addressing some of the major challenges I just mentioned seems quite obvious.

Take the environment challenges with, for instance, the ocean and the hydrosphere whether as an area for decarbonization, or as a carbon sink, or as an ecosystem needing serious regeneration of biodiversity. We still have a big science gap about the ocean. Building a digital twin of the ocean can help improve oceanographic science much faster than with conventional means; it's about collecting much more data with much pore precision from both space observation and water systems and then powering new simulation systems with artificial intelligence.

Take health. We know that here again, more precise data and more artificial intelligence will help inventing new laser like treatments of diseases and even more important, much better collective or individual prevention, including, in the case of pandemics.

Take food production where productivity and the impact on the environment can be vastly improved by digital systems, piloting the quantity and the timing of fertilizers usage, as well as getting rid of pests with digitally directed tools to spread bio-organisms.

Finally, and to keep my list short and leaving aside the energy, mobility and many other economic sectors, take education and professional training, which in my own experience is the number one issue, if we want to reduce social and economic inequalities. More affordable, more accessible digital devices enhance interactions and learning. They allow individual, tailor made, upskilling programs and cultural exchanges, dialogues and knowledge including of how and why others differ. They allow our mental differences to be bridged, hence reducing antagonism based on differences which anthropology tells us has been a driving force of human tensions and conflicts for ages.

For all these reasons,

> **Tech and in particular digitalization is the way to go to avoid a growing fragmentation, which I see coming in the future.** ”

But for tech to be the solution, let's make sure it does not contribute to the problem as the use of digital technology can also be a new source of divisions. Why? Because of this new complex digital nexus between technology, security and ideology which has appeared in the new non-material part of the economy. While artifacts are usually ideologically, culturally, politically neutral (I mean, a car is a car, everywhere on this planet), data systems are not neutral. It's also different in the digital area where cyber penetration is a much higher threat in the new economy than the old one. These are some of the reasons why data collection, accessibility, storage, privacy, and cross-border circulation are regulated differently in different places. Thus, progressively creating a much more unlevel playing field with its inevitable loss of economies of scale and hence loss of efficiencies and hence loss of welfare potential. A sort of digital non-globalization in the making.

This is why I believe we need to seriously consider how to shape the global governance of our digital ecosystems, and how to frame local regulations in a way that keeps as much openness as possible to the benefit of free exchange.

While areas like accessibility or privacy will inevitably lead to divergences, let's try and keep the necessary interoperability in order to organize coexistence. On the other end of the spectrum, where convergence is still possible, such as on the security or the resilience of digital infrastructures, let's try and keep convergence as the guiding strategic concept. **In the case of digital trade, a global frame is being negotiated at the WTO. It is about finding the necessary balance between coexistence and convergence to address these new challenges of digital trade interdependencies. I remember from my time when I was a DG of the World Trade Organization, how the International Technology Agreement has worked, including in providing easier access to technology for many poorer countries.** It is also about allowing connected global supply chains to do what they can do best; distribute technology as efficiently and quickly as possible; to as many people as possible..

In a nutshell, and to conclude, let me share with you my conviction: growing gaps in this world are dangerous. The right response is to try and bridge them. Tech has to be one of the arches of these bridges we need to build collectively. Let's work hard to build more reciprocal trust in tech and to find the necessary compromises between our systems, knowing that this will imply trade offs, give and take, where possible. This is the very purpose of the various digital initiatives, which we have been nurturing at the Paris Peace Forum since 2018. More to come in the future!

> “ Growing gaps in this world are dangerous. The right response is to try and bridge them. Tech has to be one of the arches of these bridges we need to build collectively. ”

WORKING TOGETHER FOR A SECURE CYBERSPACE

Ken Hu
Rotating Chairman
Huawei Technologies

CYBER SECURITY REQUIRES A JOINT EFFORT

As digitalization connects the world, cybersecurity is becoming more important than ever before. In the news, we've seen an increase in cyberattacks aimed at critical infrastructure such as energy, healthcare, and transportation.

These attacks have affected the lives of millions of people around the world. According to one estimate, damages from cybercrime might reach US$6 trillion in 2021.

Meanwhile, as a result of the pandemic, people are spending more time online. And I'm sure that many people will continue to work remotely, even after the pandemic. This makes it all the more important that we do everything possible to ensure a healthy and secure cyber space.

In the public sector, new laws, regulations, and standards are being introduced on a regular basis.
In the past two years alone, 151 countries have passed more than 180 cybersecurity laws. This is incredible progress. In the telecoms sector, industry organizations like GSMA and 3GPP have been working closely with industry stakeholders to promote NESAS Security Assurance Specifications and independent certifications.

These baselines have seen wide acceptance in the industry, and we're confident that they will play an important role in the development and verification of secure networks.
However, we still have a lot of work to do. Cybersecurity is a complex, evolving challenge that requires close collaboration and information-sharing. We still lack a standards-based, coordinated approach across the industry, especially when it comes to governance, technical capabilities, certification, and collaboration.

In some places, there's still a misconception that country-of-origin affects the security of network equipment and technology. This is simply not true. It doesn't solve the real challenges our industry faces, and it prevents us from forming a unified approach.

> **"At Huawei, cybersecurity is our top priority.**

OPENNESS TRANSPARENCY COLLABORATION
HUAWEI
CYBER SECURITY TRANSPARENCY CENTRE
BRUSSELS
HUAWEI
HUAWEI CYBER SECURITY TRANSPARENCY CENTRE

We take this responsibility seriously, because we owe it to our customers – and their customers – to make sure that the equipment they're using is healthy and secure.

We're proud of what we have achieved. For the past 30 years, we have served more than 3 billion people around the world. We support the stable operations of more than 1,500 carrier networks in over 170 countries and regions.

And we have maintained a solid track record in cybersecurity this whole time.

This is the result of continuous long-term investment in cybersecurity management practices and technology for more than 20 years. We currently have more than 3,000 cybersecurity R&D personnel, with 5% of our R&D spend focused exclusively on boosting the security of our products.
Of course, our cybersecurity assurance systems weren't developed in a vacuum. They're the result of regular engagement, joint research, and joint innovation with our customers, partners, industry groups, regulators and standards organizations around the world.

That's what Cyber Security Transparency Center is all about. We opened it in Dongguan, China, in June 2021.

Two years before, we had opened a similar center in Brussels. Both Centers adhere to Huawei's ABC principle for security: "Assume nothing. Believe nobody. Check everything."

Two years before, we had opened a similar center in Brussels. Both Centers adhere to Huawei's ABC principle for security: "Assume nothing. Believe nobody. Check everything."

The idea is that both trust and distrust should be based on facts – not feelings, not speculation, and not baseless rumor. We believe that facts must be verifiable, and that verification must be based on standards. With this as our guiding principle, we've set up six cyber security and transparency centers over the past 10 years in Europe, the Middle East, and North America.

The center in Dongguan will have three main functions:

- Demonstrate solutions and share experience
- Facilitate communication and joint innovation
- Provide a platform for security testing and verification

Our most advanced center yet, it's designed to gather and serve stakeholders from around the world. It has the best tools, testing environments, and experts available for our partners, customers and industry peers. They can come to understand and test our products; and together, we can collaborate more closely on security standards, verification, and innovation.

Looking to the future, I believe we must do three things.

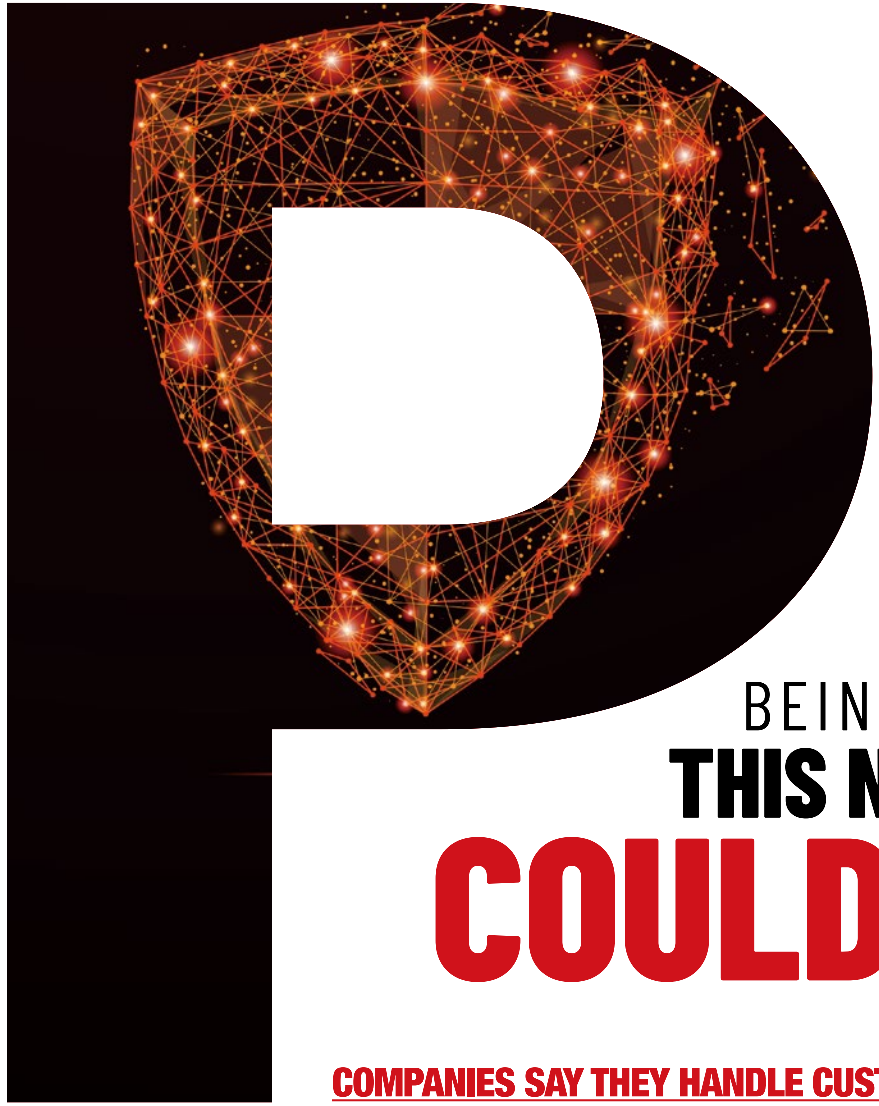
First, we must build capabilities together. Cyber security threats are complex, diverse, and evolving, and no single organization has what it takes to tackle them all. From governance, to standards and technology, to verification, we need to work together, combine strengths, and build our collective capabilities.

Second, we must share value, such as Huawei's Product Security Baseline (see related article). The more knowledge and best practices we share, the more effectively we can strengthen cybersecurity as a community.

Third, we must form tighter coalitions. That means governments, standards bodies, and technology providers need to work closer together to develop a unified understanding of cybersecurity challenges. This must be an international effort.

The bottom line is that cybersecurity risk is a shared responsibility, and we need to treat it that way. We need to set shared goals, align responsibilities, and work together to build a trustworthy digital environment that meets the challenges of today and tomorrow.

> Governments, standards bodies, and technology providers need to work closer together to develop a unified understanding of cybersecurity challenges. This must be an international effort.



Philip Heah
former Assistant CEO
Singapore's IMDA

NOT SURE YOUR DATA'S BEING PROTECTED? THIS NEW SYSTEM COULD HELP

COMPANIES SAY THEY HANDLE CUSTOMER DATA RESPONSIBLY. BUT SHOULD THESE CLAIMS BE GIVEN CREDENCE?

Philip Heah wants to answer that question in a measurable way. In September, his company, Singapore-based Credence Lab, launched a rating system that grades companies on how well they protect the data with which they are entrusted.

Credence Lab is a start-up, but its Data Trust Rating System (DTRS) was developed in consultation with some big names in technology and business strategy including Alibaba, IBM, and KPMG.

"The topic has been discussed for a long time but has not been fully addressed," says Heah, a former telecoms regulator turned entrepreneur.

Stiff penalties

Given that companies are legally required to comply with local laws such as Singapore's Personal Data Protection Act (PDPA), some might ask whether such a certification is even necessary.

Heah explains that existing certification programs are about basic legal compliance. The Credence system, by contrast, looks at a range of factors including communications, accountability, user rights, and even corporate culture.

Passed in 2012, the PDPA law originally hit violators with a fine of 1 million Singapore dollars (US$737,229). But in December 2020, the maximum penalty was stiffened to 10% of a company's local revenue – potentially as draconian as the 4% maximum fine on global revenue levied by Europe's GDPR law.

"Many companies don't have 10% profit margin," Heah notes. "Your risk exposure is extremely high."

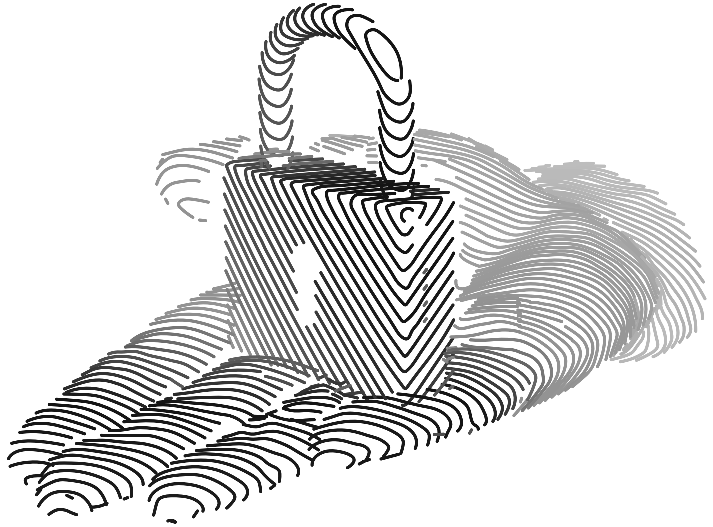
That risk can be mitigated if companies demonstrate that they understand the importance of protecting customers' data and are taking concrete steps to protect it.

> **"You can't treat data as someone else's job. It requires the attention of top management."**

Before Credence Lab certifies any customer, the company's practices are audited in several areas:

- **Corporate governance. "Does management really understand the value of data – its potential benefits and risks?" Heah asks. "You can't treat data as someone else's job. It requires the attention of top management."**
- **Data governance. Do companies understand how data comes into their organization? Have they obtained users' consent? Are they using the data for its intended purpose? Are they storing it properly, and for an appropriate length of time?**
- **Technology of Data. What kind of data protection is put in place for data, at rest and in transit? What are the security measures to protect the system, for mobile devices and media assets?**

The company's data-privacy practices are then audited by third party assessors such as TUV SUD, a German company that tests and certifies technical systems. Following that evaluation, Credence Lab confers the actual rating.



"As time passes, we can expand on the rating system to make it more comprehensive," Heah says. "Then you're not just legally compliant, but you have all the necessary controls in place – and so do your data ecosystem partners."

The weakest link

For many companies, those partners – suppliers and intermediaries – could actually constitute the weakest link in the data protection chain.

In the argot of data privacy, *controllers* receive user data and interact with users, while *intermediaries* get data from controllers. Intermediaries have fewer legal obligations than controllers, so they may be less inclined to protect data carefully.

For that reason, a company may want to contractually stipulate that any supplier it uses must meet the same data-protection standards that it meets itself.

This can be a win-win.

> **Suppliers may not want to jump through the hoops necessary to comply with the law of a single country. A more widely recognized certification like DTRS, on the other hand, could be more beneficial.**

Right now, it's early days for Credence Lab. The rating is not yet commercially available, although "five companies are piloting with us," Heah notes. One them, Experian, is a global provider of information and credit reporting services.

The pilot program tests companies by subjecting them to various controls and getting initial feedback. Pilots will conclude by mid-2022, at which point the commercial version of the service will be launched.

Singapore has about 7,000 multinational companies that Heah believes will want DTRS certification to manage their suppliers and other partners across the region.

"Singapore is a starting point," he says. "We want expand to regionally and eventually worldwide."

If it succeeds, DTRS could serve as a model for other rating systems that encourage companies to become more accountable and help build consumers' trust.

Philip Heah was the former Assistant CEO of Singapore's IMDA, where he was telecommunications sector regulator in charge of cybersecurity requirements. He was also project director for the Singapore Nationwide Broadband Network that put in place a full fiber network to all households and businesses.

Philip Heah was the former Assistant CEO of Singapore's IMDA, where he was telecommunications sector regulator in charge of cybersecurity requirements. He was also project director for the Singapore Nationwide Broadband Network that put in place a full fiber network to all households and businesses.

> Governments should sign mutual trust agreements committing them to a shared set of cyber norms – and they should be held accountable for nonconformance.

WE NEED A NEW MODEL OF CYBER ACCOUNTABILITY

COMPANIES AND GOVERNMENTS MUST BE HELD ACCOUNTABLE FOR SECURITY LAPSES

by **Staff Writer**

Widespread data breaches show clearly that a more rigorous approach to cyber security is needed. That means clearly defining requirements – and then holding companies and government employees accountable if those requirements are not met.

Here are four ways to move toward that goal:

Build on existing cyber initiatives

In May 2021, President Joe Biden signed an Executive Order (EO) on Improving the Nation's Cybersecurity. Mayer Brown, a global law firm, said the EO could "serve as a roadmap for Congressional cyber security legislation that could apply to most – if not all – of the [U.S.] private sector."

Another example: Germany's IT Security Act 2.0 lets the country's cyber security agency identify the customers of telecom operators. This allows the agency to notify victims in case of a data breach.

Enhance supply chain cybersecurity

Supply chains are vulnerable to cyber-attacks. One study found that over the past 12 months, 92% of U.S. organizations have experienced a cybersecurity breach stemming from vendor vulnerabilities. One-third of respondents said they had no way of assessing third-party vendor risk.

In response, the U.S. Department of Defense (DoD) launched a Cybersecurity Maturity Model Certification that all DoD contractors and their suppliers will be required to obtain. This model can be expanded to include companies not working for the U.S. government.

Improve global collaboration with mutual trust agreements

Cybersecurity is a global threat that must be tackled multilaterally. Governments should sign mutual trust agreements committing them to a shared set of cyber norms – and they should be held accountable for nonconformance. Private companies could also sign such agreements with customers, and with the governments of the countries where they operate.

Remember that managing cyber-risk is a shared responsibility

Everyone – from IT managers to C-suite executives – must understand the importance of accountability.

Cybersecurity procedures must be open to scrutiny so that it's clear whether requirements are being met.

Failure to meet them must result in real consequences to the offenders. For private companies – and for government employees – this could include publicly announced fines, loss of promotions and annual bonuses, as well as demotion, suspension or dismissal.

BACKROOM BARRICADE

KEEPING THE HACKER HORDES AT BAY

by **Ben Voyles**

SECURITY BASELINE FORMS BULWARK AGAINST ATTACKS

In the movies, cyberattacks are thwarted by good-looking young people pounding on keyboards in the dead of night. In real life, a successful defense requires more than one or two heroes – and more than one or two nights.

At Huawei, hundreds of people have spent more than 10 years working on ways to fortify the company's networks against attack. In doing so, it has pushed its suppliers – nearly 4,000 in all – to become more secure as well.

One tool for accomplishing this minor miracle is something called the Product Security Baseline.

The idea for the Baseline began in response to questions about network security posed by one of the company's biggest customers, Deutsche Telekom.

Every day, there are approximately 1 million cyber-attacks on Huawei's IT networks. "Hackers are always coming after us," said Mika Lauhde, Huawei's vice-president for cyber security and privacy. "As the world's largest telecom company, we're their first target."

The Product Security Baseline is a bulwark against those attacks.

At its heart, the Baseline is a massive checklist of technical requirements from customers in 170 countries. Added to that are laws, regulations, and industry best practices from jurisdictions around the world. The current version of the Baseline contains 54 different requirements split into 15 categories. That sets a high security bar for every piece of gear in the network.

The Baseline was purely internal at first, but that soon changed. The company notified its 2,000 suppliers that they, too, would need to follow the Baseline's strict rules.

This wasn't simply a matter of signing a pledge. Before a supplier could be certified as Baseline-compliant, it had to submit to a close examination of its practices.

The test was not easy: more than half the company's suppliers failed on their first try. But Huawei coached its suppliers to help them raise their security game. Although about 200 ultimately failed to make the cut, most eventually passed. Today, all of Huawei's 3,800 suppliers adhere to the Baseline standards.

This may have promoted greater cybersecurity among Huawei's competitors. Cisco launched its own baseline in 2014, and Ericsson has its own baseline requirements as well.

Huawei shares the details of the Baseline with a wide variety of partners. "After it was released in 2020, we were thinking about how to help the whole industry move forward," explained Xue Yongbo, a senior expert on cyber security and privacy protection in the Huawei supply chain. "We decided to release the Baseline document to suppliers, telecom companies, regulators, and anyone who cooperates with us."

This is more than just an overall attempt at transparency. It's also incredibly helpful to smaller telecom operators that might not have enough staff to formulate security standards of their own.

To date, the Baseline has helped Huawei earn more than 380 product security certifications from organizations around the world. Because security needs are constantly shifting, the Baseline has evolved over time, growing from 38 basic primary requirements to 54 in the latest iteration.

But in one important respect, the Baseline hasn't changed: to work with Huawei, developers need to make sure their products meet the company's standards. They must pass tests at Huawei's Independent Cyber Security Lab that certify compliance before their devices can be accepted as Huawei hardware.

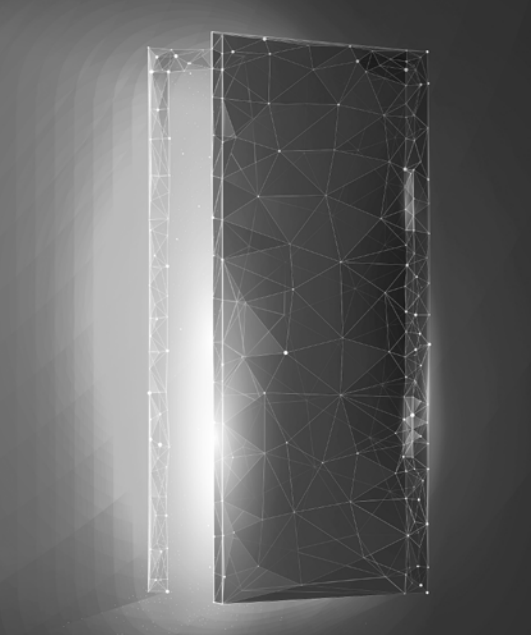
The Baseline itself is part of a larger assurance system covering verification, third-party supplier management, manufacturing, delivery, issue response, traceability, and audit – all of which must constantly adapt to a changing threat environment. The rise of remote work, software-as-a-service, and the Internet of Things create opportunities for cyber malfeasance, and most computer viruses can mutate just like their biological cousins.

Making networks more secure will only get more challenging in the years ahead. Fortunately, the ever-evolving Baseline will be ready for whatever the future brings.

The Baseline has helped Huawei earn more than 380 product security certifications from organizations around the world.

Zachary Overline
Huawei Technologies

Scan QR code
to watch the full video



WHAT DO YOU MEAN "BACKDOOR"?

When you hear about Huawei in the news these days, you hear the word "backdoor" a lot. But what is a backdoor, really?

It's really frustrating. A lot of people really love this word, but I find that the people who use it the most, and they use it the loudest, they're really not the ones who understand technology all that well. They like it because it sounds scary. It catches attention. But the problem is, **if you use the word back door for any cyber security threat, as a catch-all term, it dumbs down the conversation, while ignoring some pretty basic facts.**

Yes, backdoors are bad. So let's talk about them: what they are, what they do. And let's talk about other types of network doors too, because people tend to confuse them. There are three types.

So the first type of "backdoor" is actually a front door. It's called "Lawful Interception."

As the name implies, these are legal doors for governments to intercept network communications – basically wiretapping. In most countries, operators are required by law to install these doors in their networks for law enforcement purposes, and it can be a good thing.

Say there's a terror threat, or the FBI is building their case against a dangerous criminal. With proper legal authorization – usually a court order – lawful interception gives authorities access to the communications and data traffic of that criminal.

This type of access is all above board, or at least should be. In almost every country around the world, including the U.S., governments require operators to install these types of access points should the need arise. This brings me to a major point: transparency. From a cyber-security perspective, a true backdoor is hidden, and used for unauthorized access.

The existence of lawful interception is completely transparent and authorized. There are public standards for it. It's no secret. There's an organization called 3GPP. They're the international standards organization that sets all the technical standards for network communications and network equipment, and the specifications are right up on their website.

So if law enforcement gets a court order to use the front door, who uses the back?

Sometimes service providers are given special access to the network. But this isn't backdoor access, because it's authorized and known.

This second type of door is more like a workman's entrance. It's used to set up, maintain, upgrade and repair the network. A service door.

You know, telecom operators in the U.S. are legally required to meet a reliability standard called the "Five Nines." That means the network has to be up and running 99.999% of the time.

That's a pretty high standard. To meet it, when a network needs maintenance, the operators give equipment vendors like Huawei special one-time, limited access to the service door.

This is only done with the permission of the operator, and under very strict oversight. So it's transparent.

We have specially configured laptops that log every keystroke our engineers make. So there's a record of everything we do while we're maintaining the network.

The use of these service doors is very, very strictly monitored, and they have their own special ways of detecting any funny business.

Now for the third type. The real sneaky backdoor.

This is the true meaning of the term: a vulnerability – installed either on purpose, or by accident – that can be exploited by bad actors.

They aren't really at the back of the network. They could be anywhere, and take any size or any shape.

Edward Snowden blew the whistle on this type of backdoor in 2013, when he revealed that the U.S. National Security Agency pressures some companies to install vulnerabilities in their products. These backdoors allow the N.S.A to circumvent security protocols, and get access to otherwise private information.

So does Huawei install these? Hell, no.

Take all that noise that you hear in the news, put it aside for a few minutes and think about this: the security of our products is our bread and butter.

If anyone ever found a malicious backdoor in our equipment, every single carrier around the world would drop us in a heartbeat.

This company, that we spent 30 years building, pouring our hearts in it, our souls in it – that supports the lives of 194,000 employees and their families around the world – would be gone overnight, forever.

We wouldn't risk that. But you don't have to take our word for it. For the past eight years, Huawei has provided its hardware and software to the National Cyber Security Center in the U.K. for really in-depth inspection. The National Cyber Security Center is where you're going to find the top cyber security experts in the U.K., if not the world. They answer to the G.C.H.Q., which is basically the U.K. equivalent of the N.S.A.

They take Huawei's technology and rip it down to the bones, and they perform physical checks of the equipment, and digital checks of the software. They go through our code line by line, bit by bit, looking for any evidence of vulnerabilities.

And guess what? They have found areas where we need to improve our engineering processes. But at the same time, **the best cyber security experts in the U.K. have concluded that there's no evidence of malicious backdoors or state interference in Huawei equipment.**

This is publicly available information. And then on the customer side, before they install our equipment on the network, they test it extensively. And then, once everything's up and running, they scan it continuously to make sure that there's nothing suspicious going on.

Look, in the past 30 years, no one has ever found a single shred of evidence that Huawei has ever installed a malicious backdoor in its equipment – literally, not even once.

It's really good that people are talking about cyber security. But we need to be clear about what we're talking about, and honest too.

Because if we use our words too loosely, it makes it really hard to agree about what a secure, strong network should be.

So, the next time you hear somebody throwing these words around, and it feels like they're trying to ramp up a little bit of fear, why not push back a little. Ask them: What do you mean by "backdoor"?

Transform | HUAWEI

**“In the next issue,
we look at the subject of resilience.”**

🌐 Visit us at www.huawei.com/en/facts/transform

✉ Contact us via gavin.allen@huawei.com