Jason Woodson,
Principal Network Security Engineer @ NTT
jason [dot] woodson [at] gmail [dot] com
My third time presenting at RSS

Information for this presentation was pulled from headlines, books, industry reports, govt statistics, academic papers, security experts, think tanks, govt officials, and privacy rights groups. References at the end

---

I. Data breaches are devastating to people and our communities.
High profile breaches make headlines - Equifax, Target, Home Depot
But the people who are ultimately victimized, that doesn't make the news

II. There are people, companies, organizations, and other powerful interests who either allow data breaches or outright profit from it
We're going to look at some of them

III. What can we as citizens do?
We should be fighting for data privacy as a human right
The US has a long history of

safety, and consumer protections against powerful interests

We can turn the tide

We've seen these numbers, they are grim

Breach fatigue

Vendors use them to scare us into buying their products

But let's understand that behind every record breached there is a real person

US pop is 327m

The Identity Theft Resource Center
Non-profit organization that provides consumer education and free assistance to victims of identity theft.
Consider a donation.

In 2016 they released a report, Identity Theft: The Aftermath.
The report is a survey of over 300 victims from 40 states.

One of the most striking findings
More than half of the respondents had household incomes of less than $50,000 annually. Disproportionate impact, these victims are less able to deal with the resulting expenses and other challenges.
Domino effect, devastating to the most vulnerable

Criminal ID Theft - crimes committed in their name resulting in a warrant for their arrest,
criminal conviction under their name,
booking as their name,
or a criminal giving their info to law enforcement.

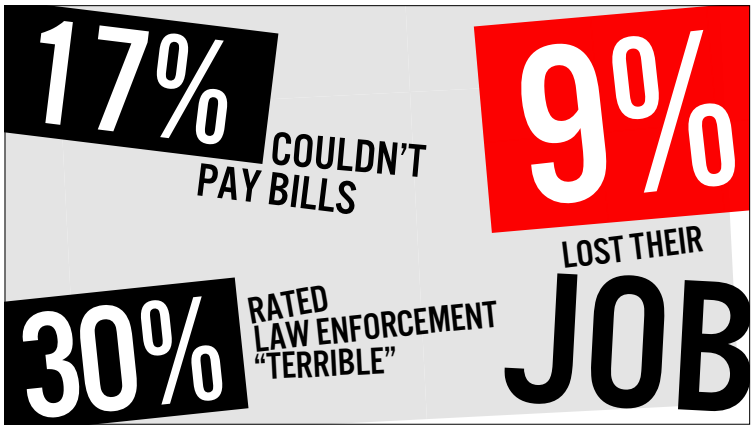
Medical Fraud -
billed for services not received
insurance company contact about service they didn't receive
prescriptions obtained in their name
doctor asking about a visit that didn't happen

Govt Identity Theft - which includes taxes filed in their name, drivers license obtained in their name, or their ssn used for work.

New Account Fraud - where a criminal opened a new account for a phone, internet service, bank account, loan, or credit card using the victim's identity.

Govt assistance - impacts us all (taxes)
More asked friends and family for assistance
40h - that and $1343 harder for lower income people. disproportionate impact

---



Behind every individual record stolen in a data breach is a real person
Data breaches harm our communities - us, our families, our friends, our neighbors, our coworkers, and people we interact with every day.
Let's look at some examples

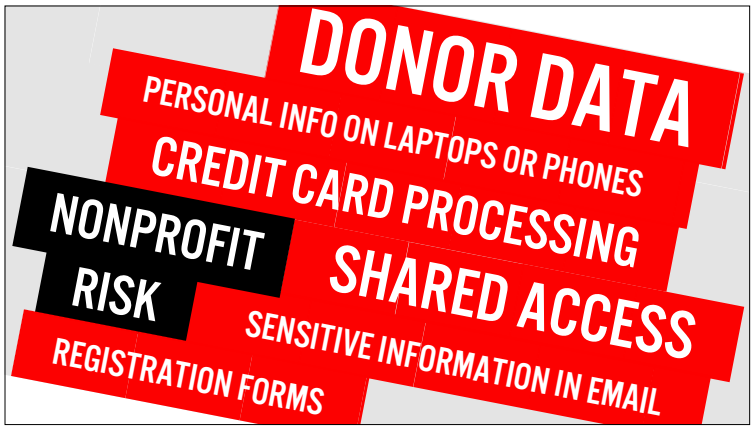
Vulnerable
Impact on parents
Children may have to deal with the fallout as they grow older
A growing trend

Bruggers Bagels major breach in 2018 (Rochester)

High remediation costs for a small business

A third of customers will stop business with a small biz after a data breach

---



- Nonprofits have similar risks to retail
- Local nonprofit xxxxxx (Rochester) breach march 2019. Senior living, mental health housing. SSNs exposed. Again, some of the most vulnerable
- Places of worship, churches, at risk and seeing impact

What chance does my small town govt have against highly organized criminals and nation-states (North Korea, Iran, China, Russia, etc)?
2011 Town of Pittsford (Rochester suburb) hacked, $139,000

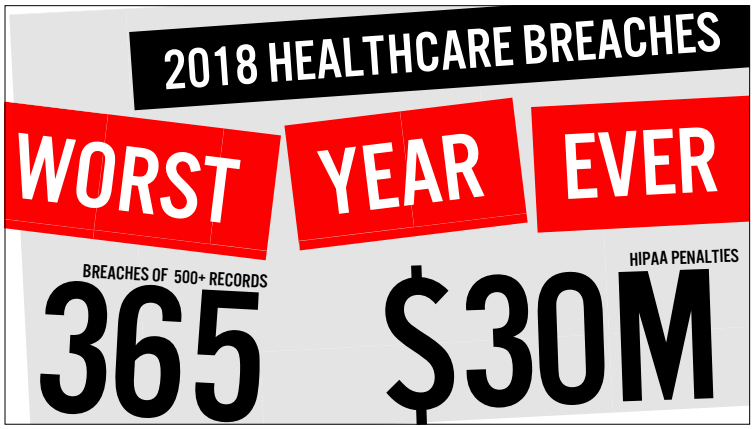
Recent streak of ransomware has had major impact on local govt
Government emails were down
911 dispatch systems were taken offline.
payments to city departments couldn't be made online.
Tickets couldn't be paid.
Utilities were double-billed.
Real estate transactions couldn't be processed, leaving some home sales in limbo.
court cases rescheduled,
Police submitted reports on paper.
Domino effect and disproportionate impact for lower-income citizens

---

Our local K-12 schools are frequently targeted

And counting.
- Aug 2019 data breach impacted several Rochester, NY-area schools in the news

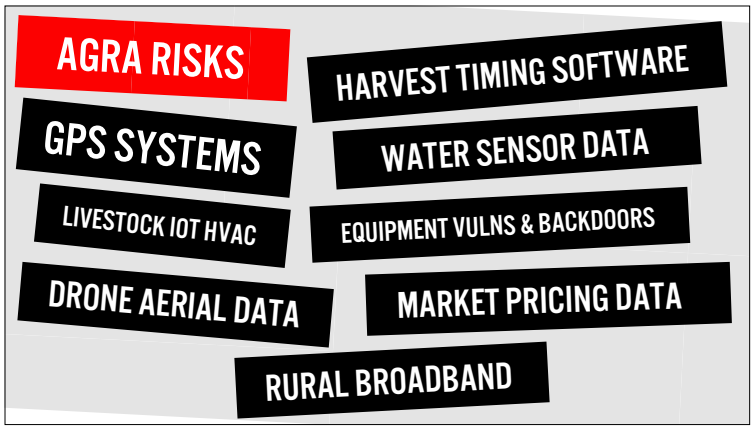
---



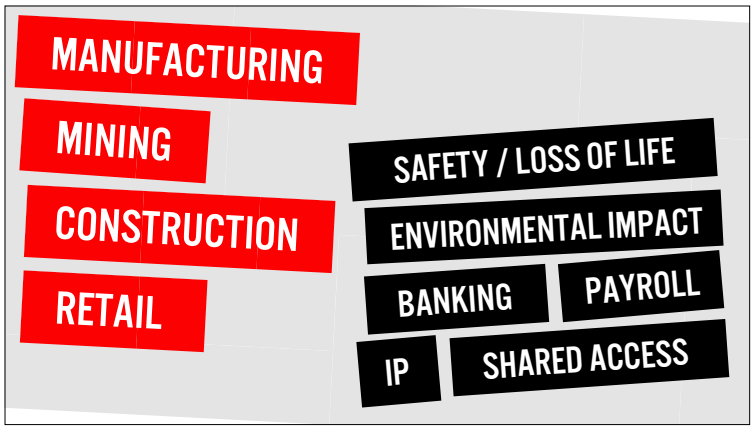
Our local healthcare/hospitals
Statistical worst year on record for # breaches, penalties
URMC (Rochester) lists data breach notifications on their website

---

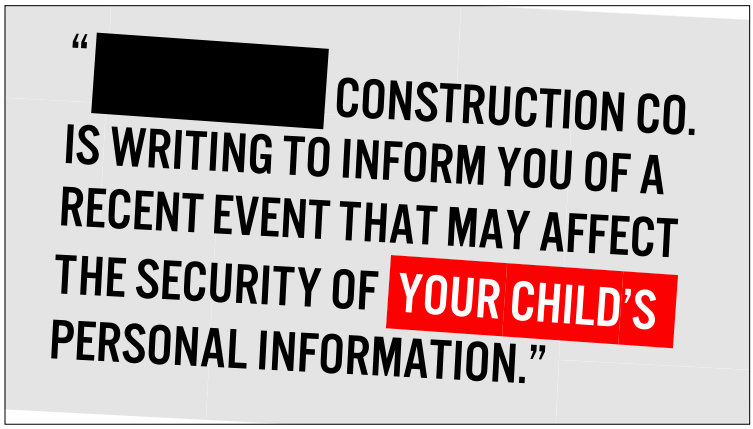
Most farms are small and family owned



Farms aren't old fashioned barns and tractors anymore
High level of risk and impact



Impacts blue-collar working-class people
High degree of automation systems
Intellectual Property



Victimizes working-class people in our communities
Not the kind of letter you want to receive
Again, the trend of child ID theft
Many reports on the high level of data breach impact on these industries

---

Beyond data breaches and the risk of ID theft, the threat of cyberwar impacts us as citizens
Three points in a timeline: 2010, 2014, 2018

US far more connected - and therefore far more vulnerable - than any other country.

Doom-and-gloom forecast any cyber attack targeting our utilities, infrastructure, power grid, or financial systems, that it would be our civilian populations and privately owned business that would suffer

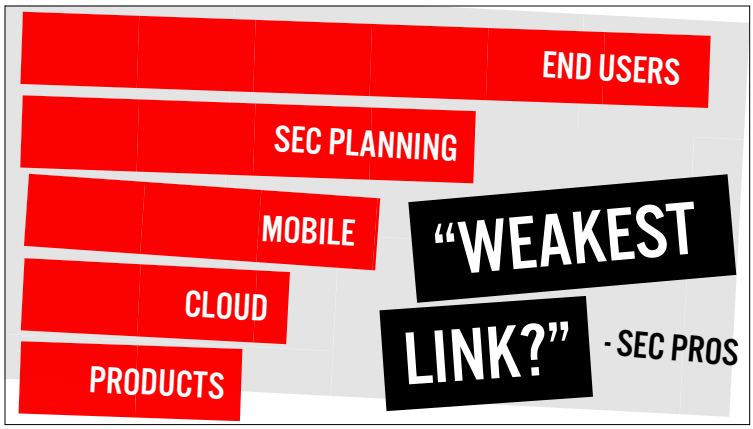
US and Israel’s (though still denied) attack on Iranian nuclear centrifuges using Stuxnet, “the world’s first digital weapon.”
underground markets where zero days sell for as much as $200,000
thriving gray market where exploits are sold to government cyber armies and spies, often foreign

---

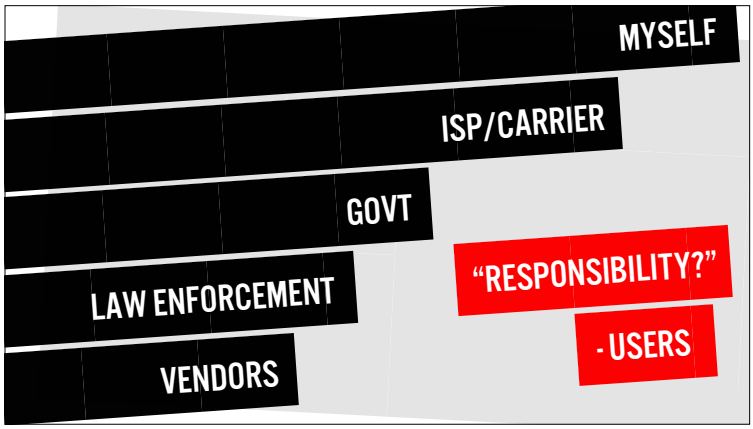
2016 election
They didn’t hack voting machines but they initiated unprecedented campaign to influence the election
Fake news, misinformation, disinformation, fake events, sensational images (candidate with Satan)
Overwhelmingly in favor of one candidate
Reached 126 million Facebook users and saw 288 million Twitter impressions.
DNC hack with leak of emails
Author considers this possibly the “Cyber Pearl Harbor” we’ve all been afraid of

---

As citizens, who can we hold responsible?



Black Hat Conference 2015 survey
Security pros blame end users



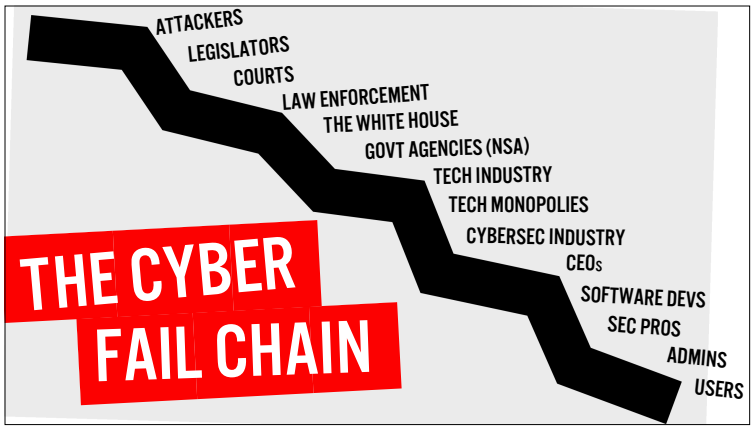
We as users even blame ourselves, even in the face of attacks from professional cyber criminals and nation states
"Who has the responsibility for your data privacy?"
Palo Alto Networks survey

This cartoon has made the rounds. I get it, but I have a problem with it and with the mantra "users are the weakest link"

You're just Dave, an overweight, balding, and incompetent Human Error in socks and sandals, staring off into oblivion, so stupid even a $125bn/yr cybersecurity industry can't help you. If you get hacked it's probably because you clicked the wrong thing or didn't install a patch. You're a (L)user, It's your own fault, and you deserve to get hacked.

It deflects blame and got me thinking - who else benefits from deflecting blame?

We've been conditioned to blame end users - the mantra is intentional

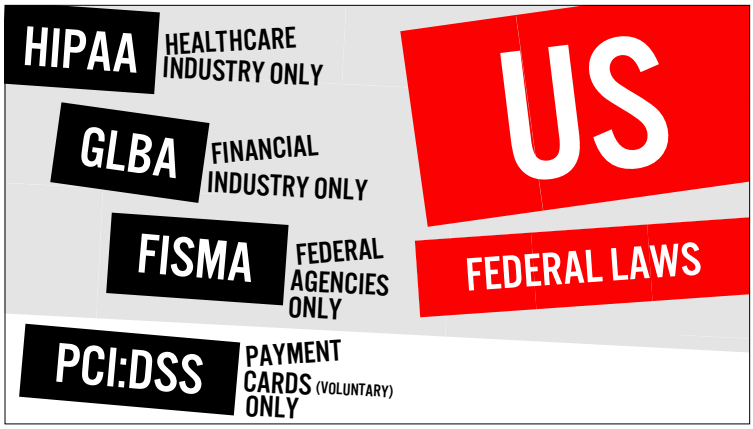


If you take away one thing it should be this
Take a photo
You've heard of the Cyber Kill Chain, this is the Cyber Fail Chain
Responsibility falls to users and admins only because so many others failed their responsibility

---

It starts with the attackers
Fair to blame them
There are different types of attackers with different motives

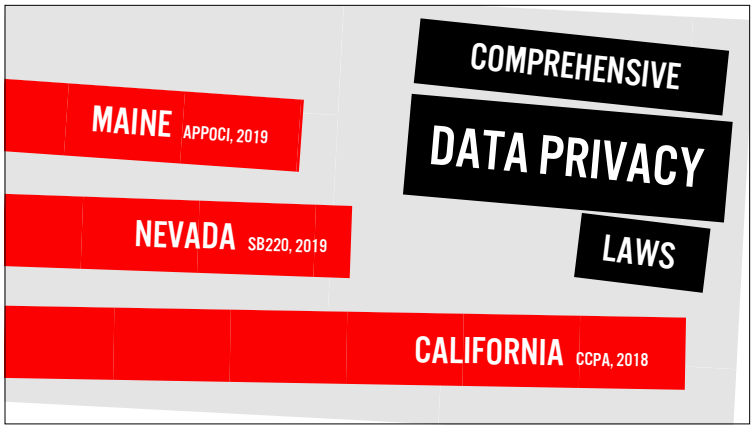
---



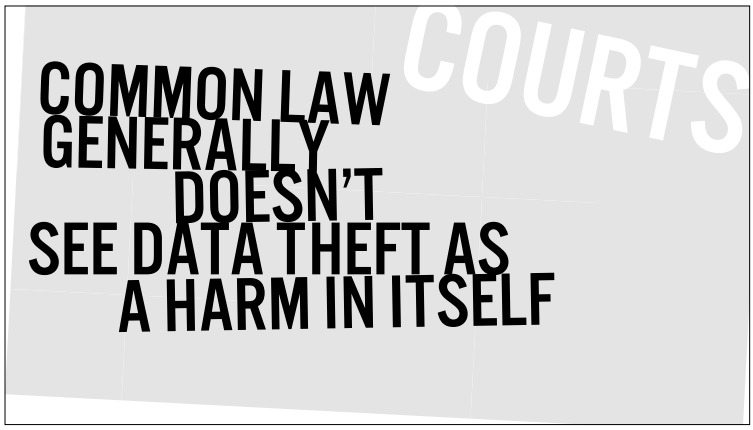
We can blame legislators
US fed laws are few, narrow, and relatively weak
Typically only require a "reasonable level of security"
Written with vague language leaving room for interpretation
"Checking the box" for compliance instead of true security
Often requires only development of guidelines and policies
Not comprehensive
Lags much of the rest of the world

So that's good

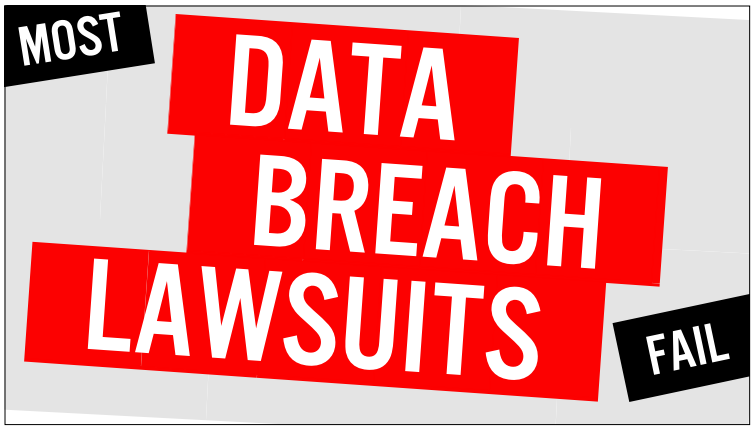
So that's good, but these laws are not comprehensive



Only 3 states have "comprehensive" data privacy laws, all within the last year Maine and Nevada not that comprehensive

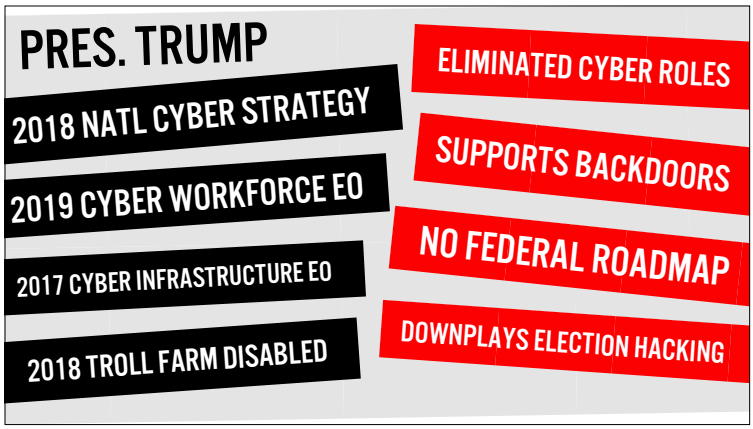


We can blame the legal system
Victims have been unable to prove that they suffered financially directly from a data breach incident. It's hard to prove exactly which breach led to harm (ie, identity theft) - the data could have come from a breach at a different company.



We can blame law enforcement.
Rate is likely lower than .1%
Many indictments involve foreign individuals and the US is often nearly powerless to enforce charges (ie, arrest).
However, this may limit their ability to travel internationally which may hinder their operations.
Attribution is a problem
Skills shortage is a problem

Facebook fine was a slap on the wrist
Projected 2019 revenue

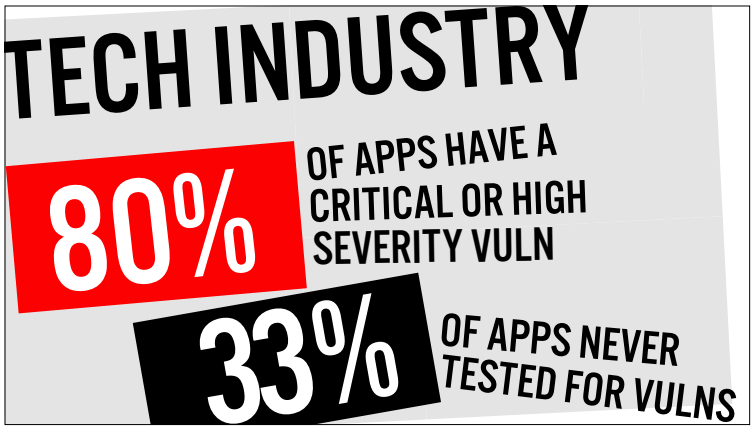


We can blame the white house (W, Obama, Trump)
Pres Trump mixed record on cyber so far
Black bars are good developments, red bars are not good
Strategy is continuation of Obama and W
Signed some good EOs
Troll farm attack was cool imo

(controversial
Eliminated White House cybersecurity coordinator.
Eliminated cyber diplomat position at State Dept
“It also could be somebody sitting on their bed that weighs 400 pounds, okay?”

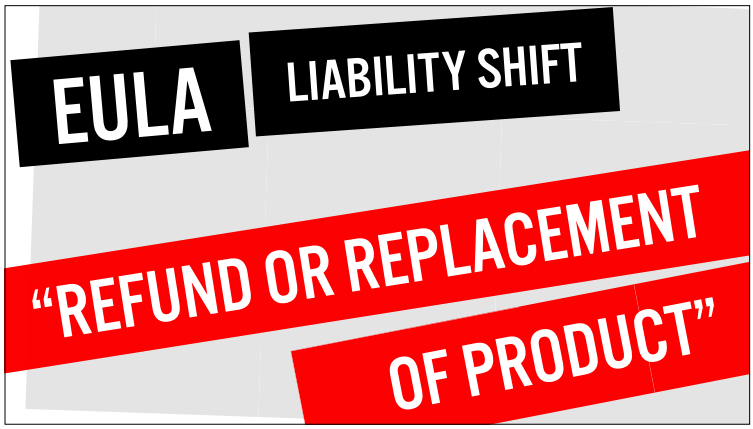
US is hacking other countries and doesn’t want to make a big deal about other countries hacking us, doesn’t want to make rules (yet)

NSA held on to the vuln for 5 years, didn’t report it to get fixed
Many victims were hospitals and schools (again, some of the most vulnerable people), Impacted many industries including manufacturing, government, and telecom
US policy “we don’t hoard zero days”



We can blame the Tech Industry
IoT devices, mobile, apps, etc

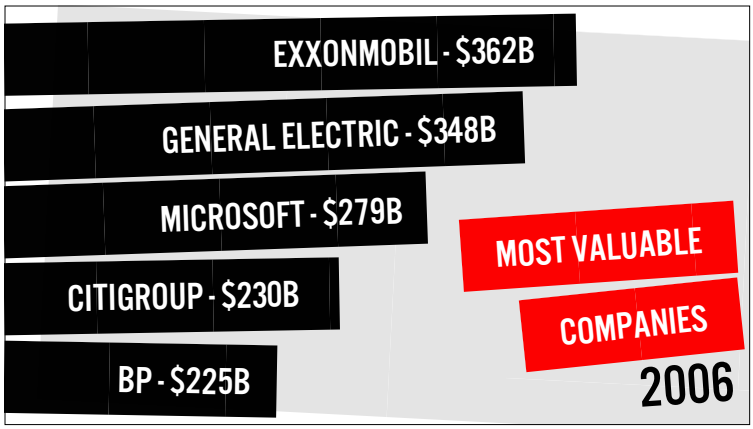
Ship!
First to market
Sec is an afterthought at best



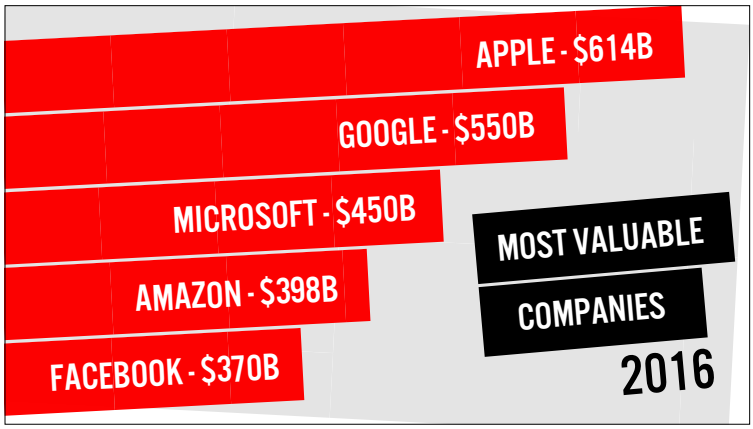
If you get hacked, Microsoft will refund or replace Windows for you
kind of a joke

Non-profit think tank
"Systemic Problems in the Software Development Landscape"

We can blame Big Tech
AKA tech monopolies

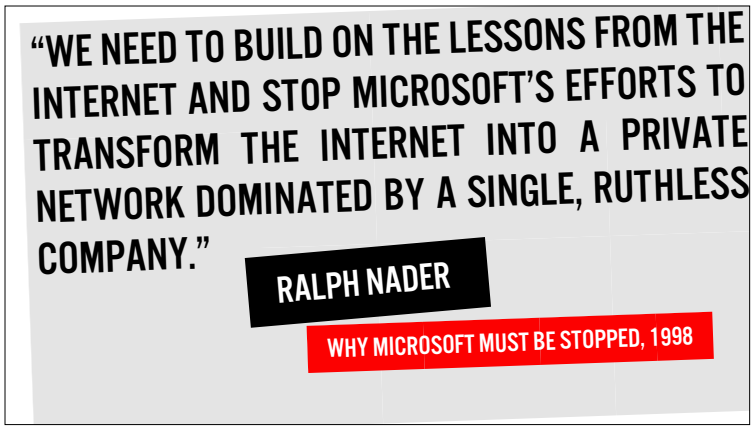


World's biggest companies change from 2006 vs 2016
From "Move Fast and Break Things" by Jonathan Taplin

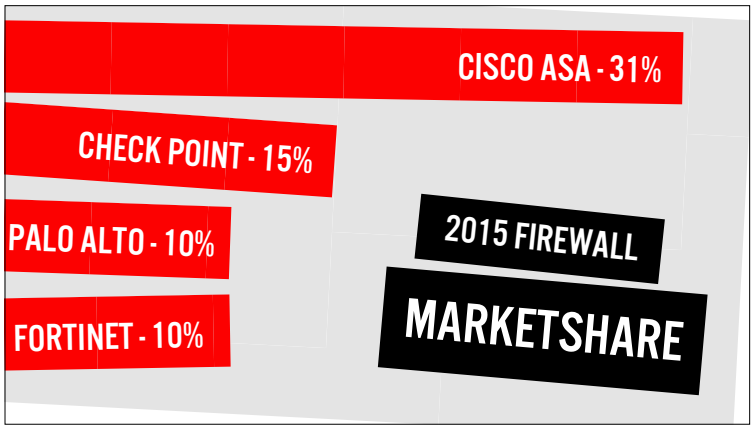


Got so big so fast
What does this mean for cyber?
No incentive to innovate or secure

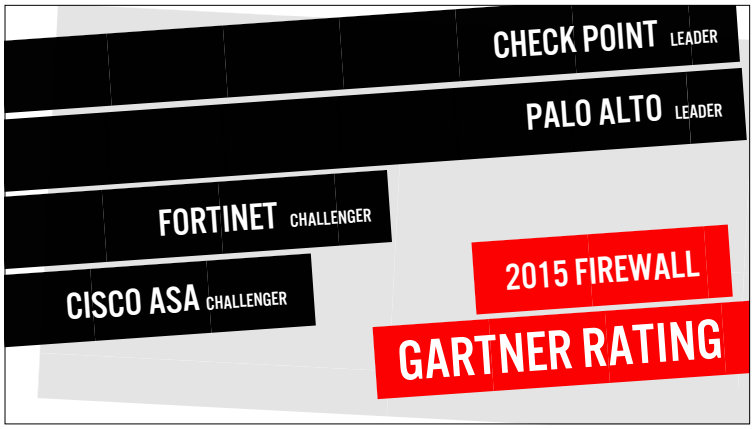
Initial judgement was to break up Microsoft, appealed and reversed
We used to say:
"Bill Gates is only good at marketing, not good products"
"Nobody has a choice but to use MS"
"MS doesn't care about security - they have no competition so what do they care"
We used to put the dollar sign in Micro$oft
MS building vulnerable software and then selling you security services, seems unethical
Still today almost 80% market share



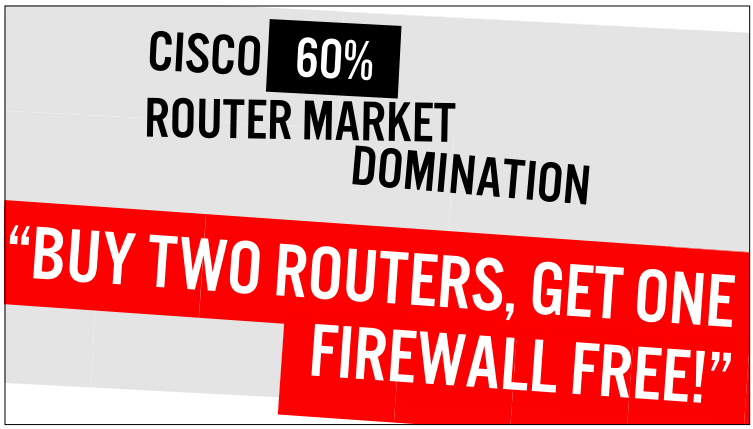
Ralph Nader - Public safety advocate, activist, writer, lecturer, reformer, presidential candidate
words are true 21 years later
Facebook didn't exist in 1998
Google and Amazon were small in 1998 - just "search engine" and "online books"
Apple didn't have iphone, ipads, or even ipods yet. Small niche player in 1998



Cisco ASA firewall dominates the FW market



Does ASA dominate because it's the best?
No, it's not the best firewall



Cisco domination of router & switch market led to ASA being installed everywhere
Which led to poor security
For many years ASA was a glorified router
Directly impacting our private data since these are installed around the world

There is no “free market” to fix this
The “invisible hand” won’t fix this
We can’t “vote with our dollars”
You can’t get away from FB if you wanted to

We can blame the cyber security industry
A massive market
Yet things still get worse year by year
Problems aren’t getting solved

Malcolm Harkins - Cymatic, Cylance, Intel, speaker, writer
There’s an inherent conflict of interest - cyber companies don’t actually want to fix the problem.
If problem was fixed, we’d all be out of a job
Malcolm Harkins -“The Rise of the Cyber Industrial Complex”

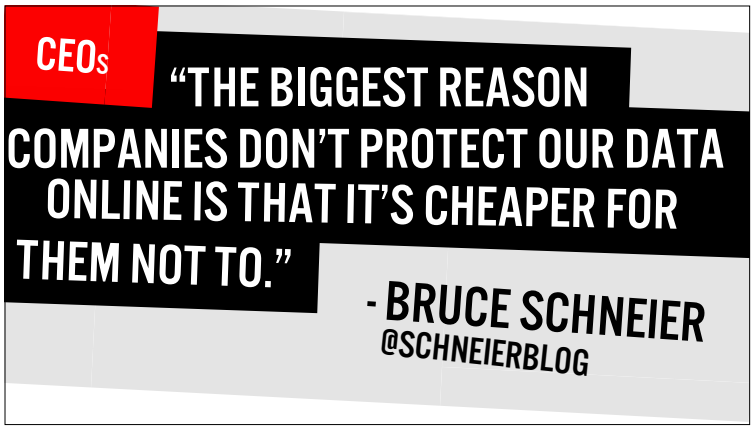
Cyber insurance, interesting development, since insurance companies are denying claims because companies aren’t following sec best practices. May end up driving sec innovation

We can blame software developers (programmers)
Software they write are vulnerable to exploits
Devs aren't trained or hired for sec skills

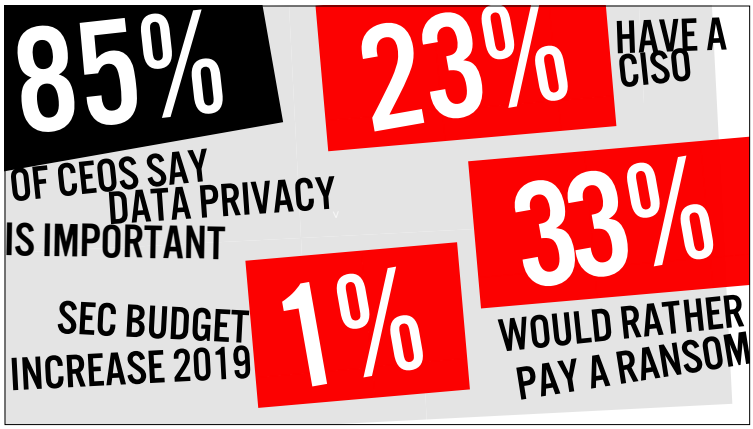
Half of developers say there isn't time for security
IT decision makers say sec and net are not in close enough contact
Not all Devops treat sec as a hindrance but it's common

Hey, it's possible. just cost money
Medical devices have higher standards required. So it's possible

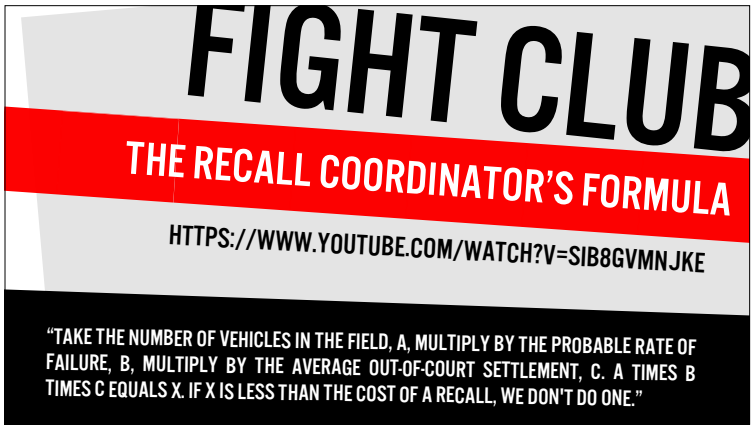
---



We can blame CEOs
If you take away two things - this one too. Take a photo
CEOs want 4 new rolexes, not just 3
Bruce - cryptographer, computer security professional, privacy specialist, writer, former RSS Keynote



CEOs talk the talk but don't walk the walk



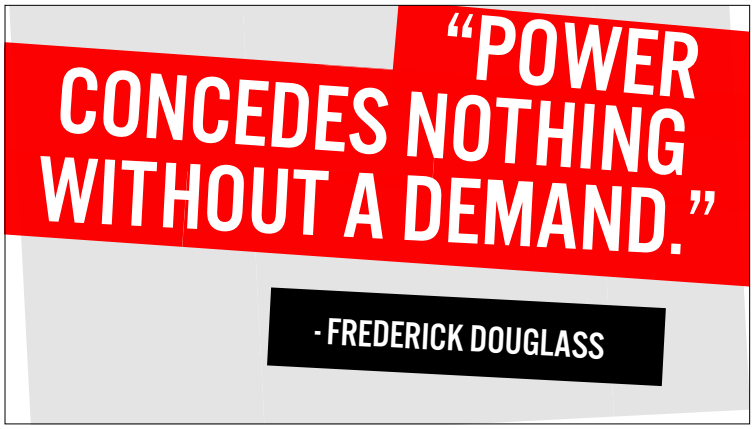
This video is basically the current state of cyber security.

We can blame CISOs and sec pros
I've seen it first hand - Techs and executives speak different languages

Sec pros deflect blame to end users and don't take responsibility
Ira - sec pro, speaker, former DoD, former RSS keynote

Sec pros are trained to consider only monetary cost

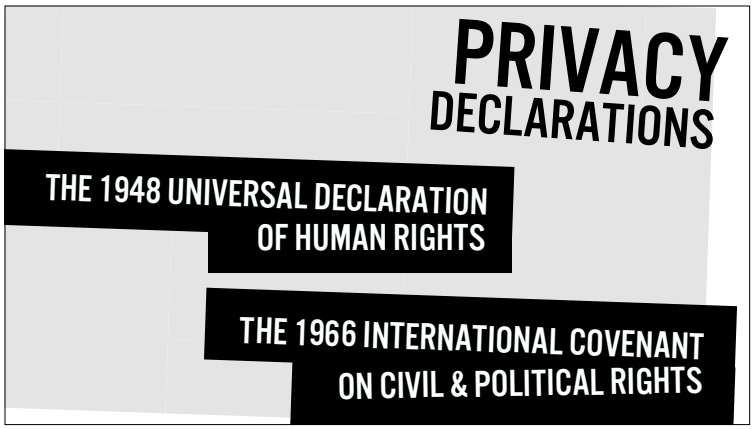
what can we as citizens do about data breaches?
a 12-step program



Data privacy is a struggle between citizens and powerful interests

---

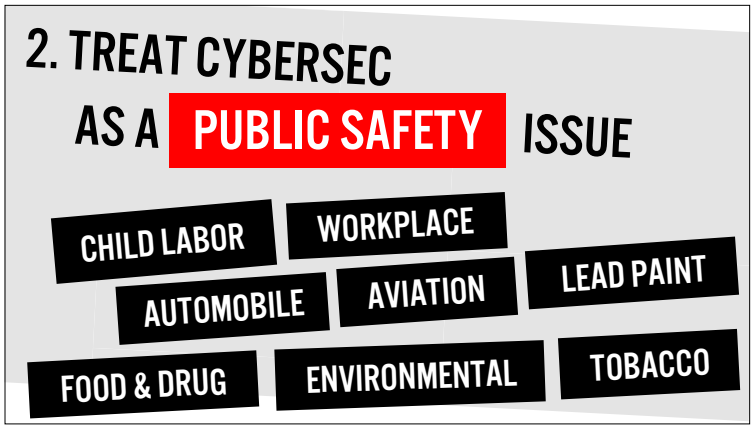
Acknowledge that data breaches have a real human cost
Humans have a right to not have their personal data stolen and used against them
This will push responsibility up
Change the narrative



Two major international declarations of privacy as a human right

---

Many other quotes



Americans have a long history of citizens fighting for public safety and human rights against powerful interests

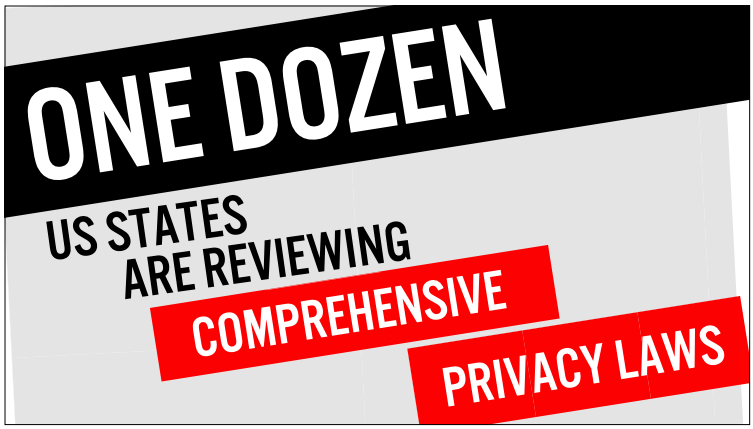
---

Manufacturers ignored safety concerns tire pressure, swing-axle suspension, chrome dashboards, non-standardized shift patterns, workmanship problems, opposed solutions such as seat belts and crash testing, all out of concern for cost.
car manufacturers created road safety guidelines that focused on DRIVERS (aka. users) and roads to distract from

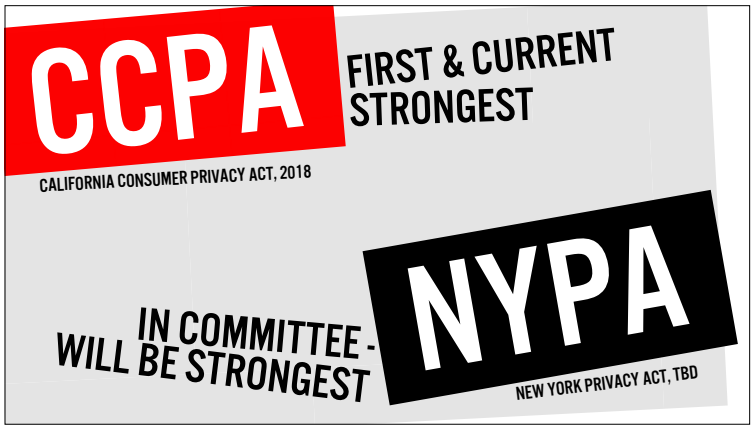
the real problems of car safety. sounds familiar

Let's not ask, let's force.
Reg - Greycastle, CIS, RSS 2019 Keynote
Pro-business guy
Greycastle talks about security ROI, sec as business (which I disagree w)
but maybe it's dawning on him (shower thought)

115th Congress, 226 pieces of legislation that focused primarily or tangentially on cybersecurity the 114th Congress introduced only 22 bills on the issue
Secure Elections Act. Kamala Harris
DETER Act - Rubio
DEFEND Act - Harris
CCCA - Gillibrand
Data Breach Prevention and Compensation Act - Warren and Warner.
IoT Cybersecurity Improvement Act of 2019 - Warner
Consumer Data Protection Act' - Sen Ron Rynden (D-OR)
ADD - Rubio
Many others



About a dozen states have comprehensive privacy laws currently under Committee review.
Only 3 so far have them as previously discussed (CA, NV, ME)



Also, In July 2019, New York signed into law the Stop Hacks and Improve Electronic Data Security Handling Act (SHIELD Act, 2019) which updates and broadens data breach enforcement laws.

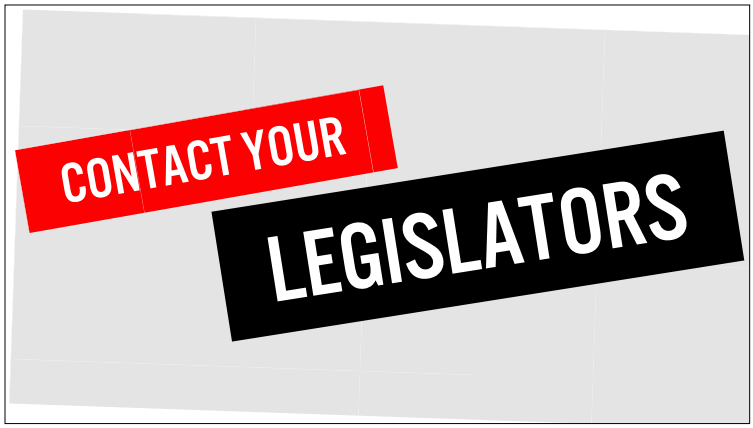
Can't talk about data privacy laws without mentioning GDPR
Most comprehensive data privacy law in the world
Many state-level US laws are GDPR-inspired
The GDPR contains key principles:
Our data can only be collected for a specific purpose
We must consent to the purpose that our data is collected
Only the data needed to achieve this purpose should be collected
Collected data must be deleted at our request or when it's no longer needed
Integrity and confidentiality
Accountability and compliance
Applies to all companies that collect, process, or hold data from users in the EU - global impact, not just EU.

Penalties as high as €20 million or 4% of annual global revenue, whichever is greater.

Proposed US state laws have many provisions in common with GDPR

Two particularly interesting provisions
Private right of action/recourse - Allowing consumers to sue
Data fiduciary - Similar to doctors and lawyers, a professional relationship. Yale Law School Professor Jack Balkin
Opposed by some for not going far enough - companies shouldn't have our data at all

---

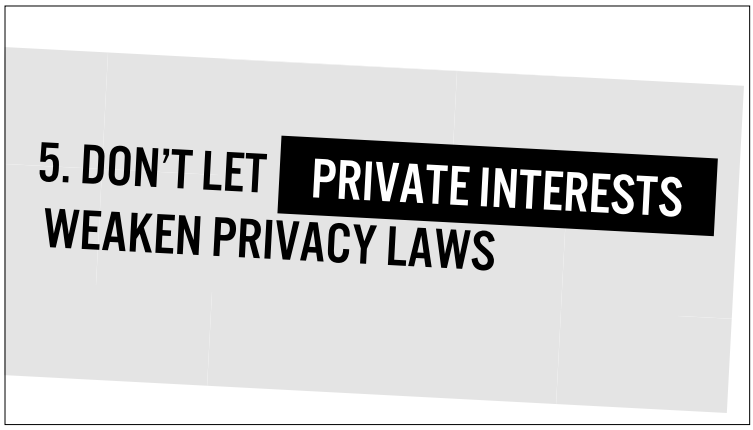


I reached out to NY Sen Rich Funke (R) via facebook to ask why he voted against the NY SHIELD Act which passed July 2019. he said local hospitals opposed the act due to overlapping requirements with hipaa and other regulations. i read the law and saw several sections that said hipaa and other regs were exempt, let him know this. he said. "that's not how i read it". i

don’t think he read it

Gilded age anti-monopoly action from 100 years ago
But brakes put on anti-trust action since the 80s
Matt - Fellow @ Open Markets Institute, writer, policy advisor, author
Lina - Academic Fellow at Columbia Law School, researcher, writer, “Amazon's Antitrust Paradox”

Very liberal and very conservative agree. Interesting!



News right now of attempts to defang current state laws
Or to pass a watered-down federal law to supersede
EFF and others raising awareness

1920s child labor laws were opposed by industry groups
Gilded Age Era trust busting, industry regulation, consumer protection, and other laws
"the progressive era"

Lobbied against. Fought installation of catalytic converters.
"no roi"

Tech lobbyists, chamber of commerce
Making it more "business friendly"
Defang, water down, take away consumer rights, reduce business obligations

---

We talked about how less that 1% of breaches have a law enforcement action

Dissuade - we saw Obama stand up to the Chinese in a rare instance and cyber attacks dropped off for months

---

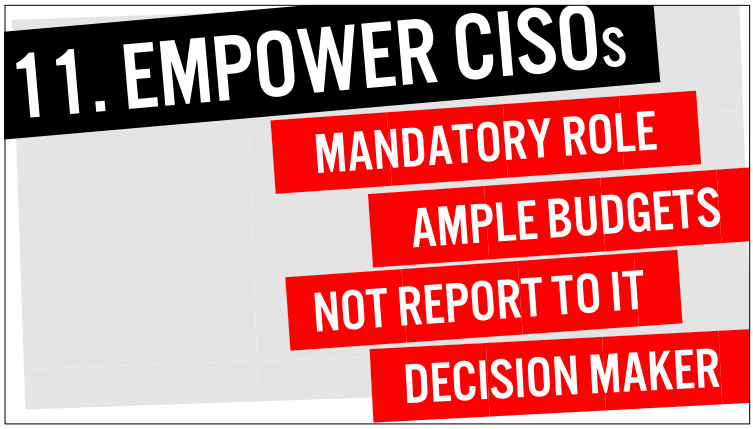
Malcolm Harkins “prevention before detection, prevention before profit”
Detection is too late
If your business model involves a violation of my data privacy, then you need a new business model.
There is no ROI with security just as there is no ROI with car safety or child labor laws.
If data privacy is a human right then just do the right thing and pony up
Companies shouldn’t be allowed to choose if they want to protect my data privacy or not

---

Security should be a crucial part of every org

If there is a breach, the victim should list all of their security controls that failed to stop it (firewall, endpoint, etc)
Vendors make wild claims. where are the warranties? guarantees?
Third party testing has done a great job lately in upholding higher quality standards
Malcom Harkins ideas

Security “shift-left” - marriage of devops and security
Kelly Shortridge @swagitda_ VP, researcher, writer, speaker, product manager, former RSS keynote
Controlled Chaos



ciso seat at the table

Stop deflecting blame and take responsibility
User risk needs to be managed
Links are made for clicking. Emails are made for opening. Apps are made for installing.
Human nature is to take the path of least resistance.
People just want to get work done.
If we treat data privacy as a human right

it will push responsibility up
Don’t allow other groups off the hook

tyty