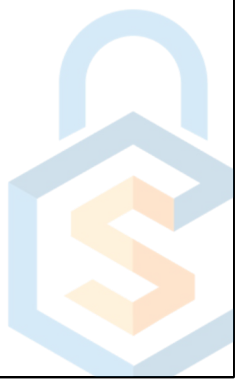
Insecure at any speed: why Secure by Design is not enough

John Benninghoff
Security Differently



Hi, I'm John Benninghoff. I started my company, Security Differently, with a goal of making cybersecurity as much a part of technology engineering as safety is part of structural engineering.

Like CISA's Secure by Design initiative, this talk was inspired by Ralph Nader's 1965 book, *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*.

I'll have a QR code at the end for you to download the slides with notes and links to all the references.

Agenda

- Auto Safety and Cybersecurity
- Secure by Design
- Why rational self-interest won't work
- Solutions by example

Agenda. Imagine traveling in a car with your mother in 1961. She starts to turn a corner…

61 Years Ago – Auto Safety

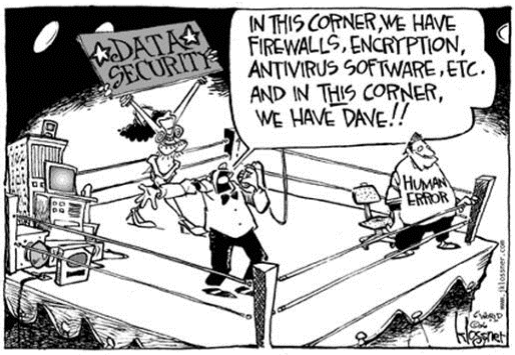
- Increasingly frequent accidents and poor systematic data collection
- Designers have the knowledge and engineering to build safe cars
- Commercial pressures prioritize features over safety
- After-market products exist to fill gaps in safety
- Drivers blamed for failures

In 1965, Ralph Nader published a surprise best seller, *Unsafe at Any Speed*, a critique of underinvestment in auto safety. Nader presented evidence that designers knew how to build safer cars, but chose not to, under the belief that "safety doesn't sell." At the time, the industry opposed federal regulation of vehicle design and emphasized individual driver responsibility for "defensive driving" and proper maintenance. The book covers many safety features that didn't exist or were uncommon at the time, that we take for granted today: seat belts, collapsable steering columns, padded dashboards, windshields, ergonomics, even airbags, antilock brakes, and adaptive cruise control! The book led to seat belt laws in 49 states (not NH), Senate hearings, and the creation of USDOT (United States Department of Transportation) and NHTSA (National Highway Traffic Safety Administration) Photo is of a 1964 Chevrolet Corvair, the first model year with improvements to an unsafe suspension design. Before then, there were after-market kits sold to stabilize handling and prevent tuck-unders.

https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed:_The_Designed-In_Dangers_of_the_American_Automobile
Image: https://commons.wikimedia.org/wiki/File:Flickr_-_DVS1mn_-_64_Chevrolet_Corvair_Monza_(3)_(cropped).jpg

Today – Cybersecurity

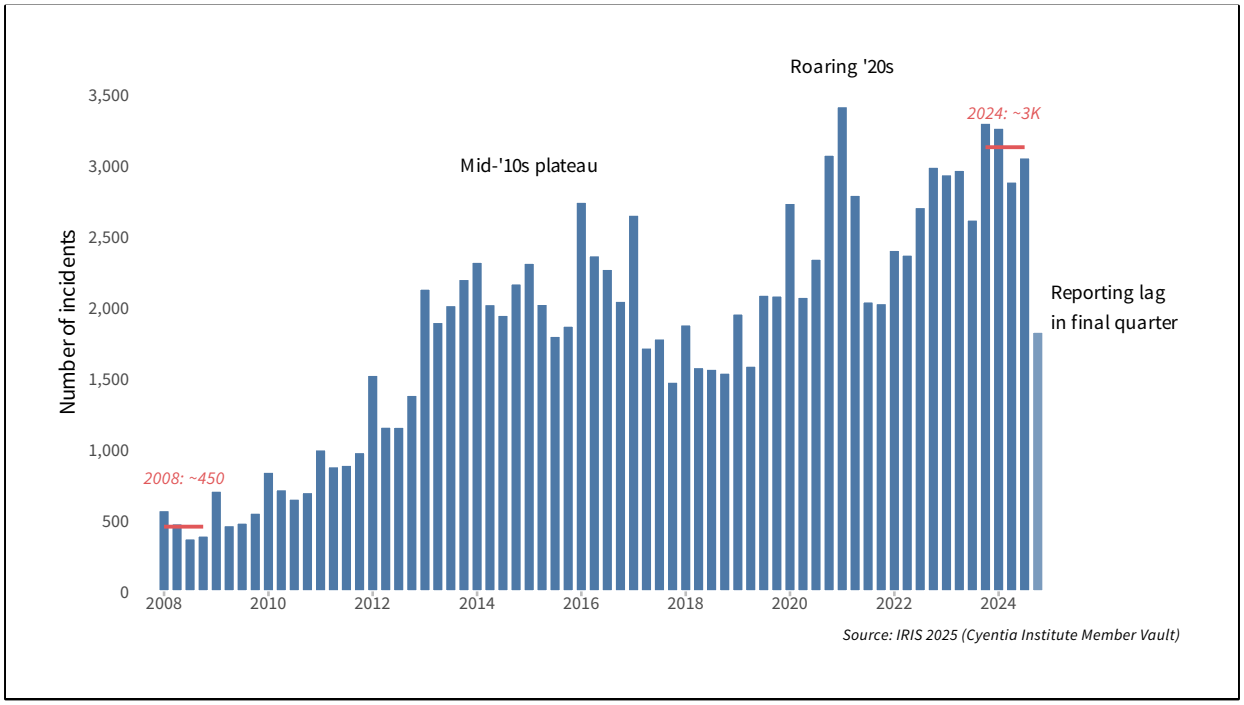
- Increasingly frequent incidents and poor systematic data collection
- Designers have the knowledge and engineering to build secure systems
- Commercial pressures prioritize features over security
- After-market products exist to fill gaps in security
- Users blamed for failures



There are remarkable parallels between the state of auto safety in the 1960s and Cybersecurity today; security incidents are increasing, and even though we have the know-how to build secure systems, there is commercial pressure to prioritize features over security. We rely on after-market products to fill gaps in security (CrowdStrike for Windows) and still blame users for security failures; the cartoon here was featured in a keynote session at a security conference I attended in 2024.

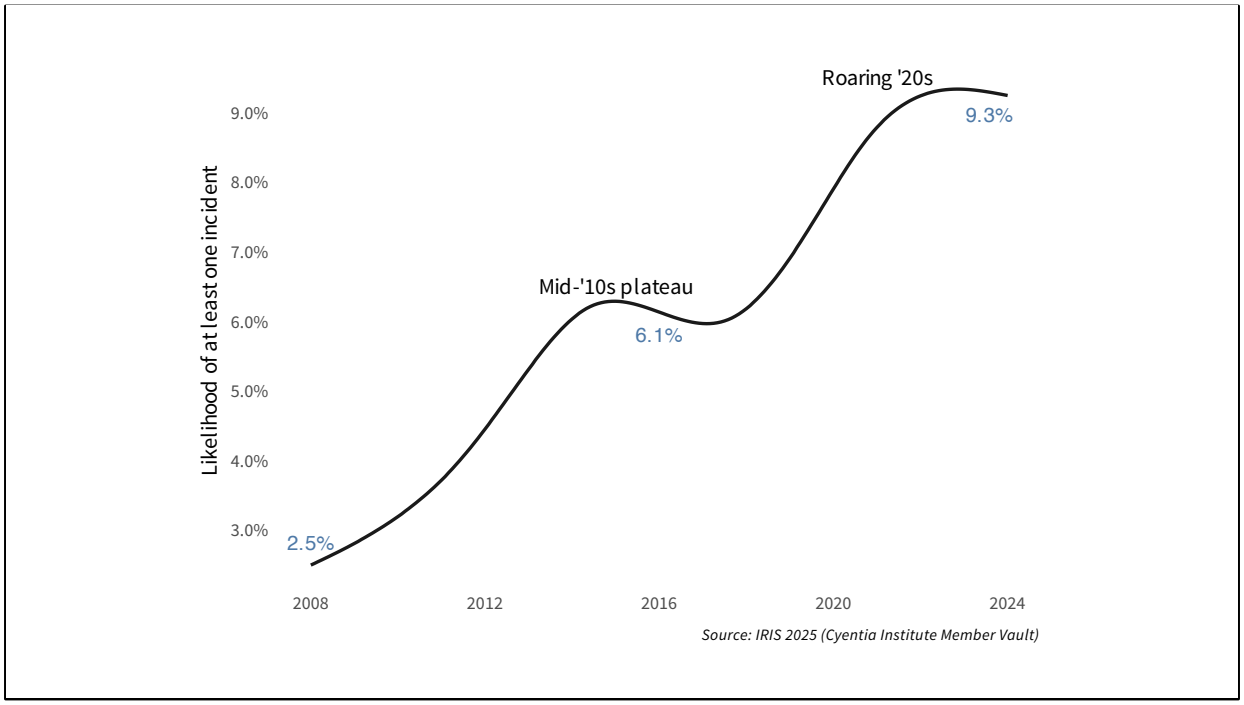
I will make the case today that improving cybersecurity requires changes in regulation and engineering practices similar to those that began in auto safety in the 1960s.

Image: https://www.jklossner.com/humannature



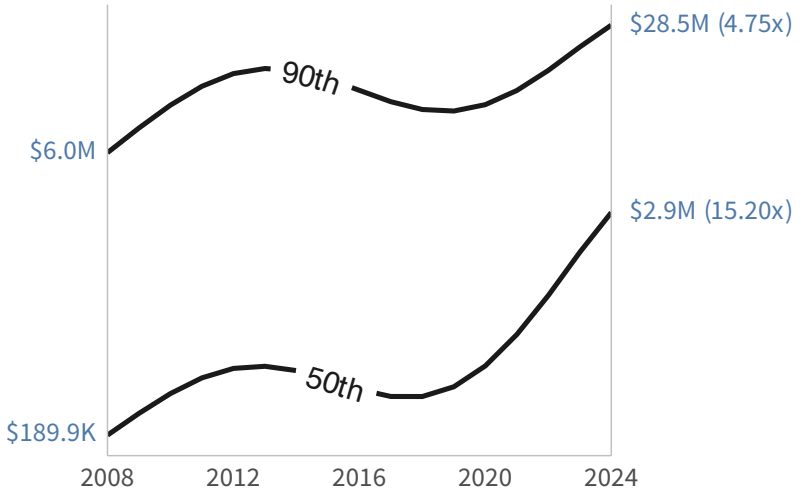
We're seeing an increasing number of incidents over time.

Cyentia Institute. (2025). *Information Risk Insights Study: It's About Time*. https://www.cyentia.com/iris2025/ (Fig 1)
Image: https://www.cyentia.com/membership-account/ (IRIS 2025 Report Figures)



The likelihood of a security incident is also increasing.

Cyentia Institute. (2025). *Information Risk Insights Study: It's About Time*. https://www.cyentia.com/iris2025/ (Fig 6)
Image: https://www.cyentia.com/membership-account/ (IRIS 2025 Report Figures)



Source: IRIS 2025 (Cyentia Institute Member Vault)

The impact of security incidents is increasing as well.

Cyentia Institute. (2025). *Information Risk Insights Study: It's About Time*. https://www.cyentia.com/iris2025/ (Fig 10)
Image: https://www.cyentia.com/membership-account/ (IRIS 2025 Report Figures)

Secure by Design (CISA)

- First paper 2023-04-13
- Voluntary pledge May 2024
- Aimed at software vendors

- Memory-safe languages
- Secure components
- Secure default configurations
- Security included (no SSO tax)

CISA, under the leadership of former Director Jen Easterly, established the Secure by Design initiative, also inspired by *Unsafe at Any Speed*. The initiative and SBD pledge called upon software vendors to improve the security of their products, and included asks like using memory-safe languages, secure hardware and software, secure configurations by default, and security features included in the base product.

https://www.youtube.com/watch?v=vkLyQcYyyTQ
https://www.youtube.com/watch?v=_n7QRuR_Tck
https://www.cisa.gov/securebydesign
https://www.cisa.gov/resources-tools/resources/secure-by-design
https://www.cisa.gov/news-events/alerts/2023/04/13/shifting-balance-cybersecurity-risk-security-design-and-default-principles

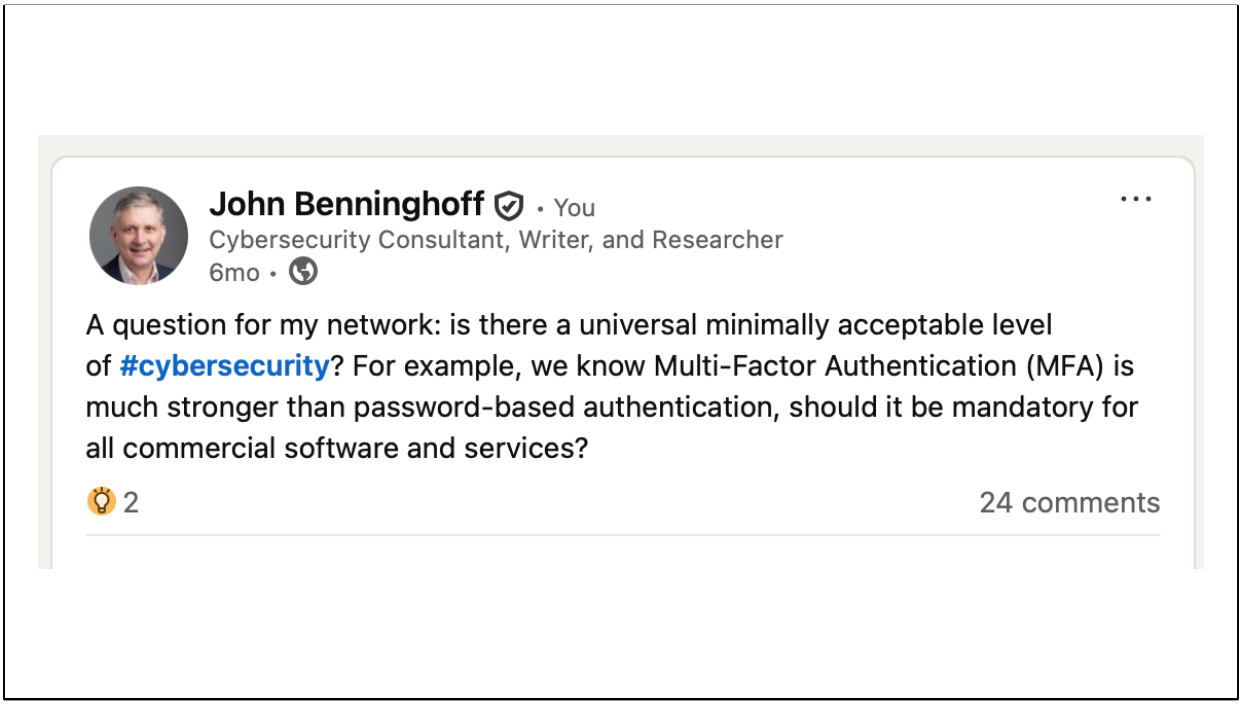
Secure by Design Progress

As of May 2026:

- 364 companies signed
- 52 provided progress reports
- 85%+ are cybersecurity and technology companies

Nearly all are either security product companies or large technology companies with presumed government contracts. Few companies not in either category. (Even Apple hasn't signed the pledge!) Basically, the orgs that signed were already committed to secure by design.

https://www.cisa.gov/securebydesign/pledge/secure-design-pledge-signers
https://www.cisa.gov/securebydesign/pledge/progress-reports



About a year ago I asked this question on LinkedIn. The consensus answer was "no", that it was a decision set by the risk tolerance of individual firms. Put more directly, firms should use risk quantification to determine the optimal level of security.

https://www.linkedin.com/posts/jbenninghoff_cybersecurity-activity-7298037514081091585-qmTe/

Managers and Externalities

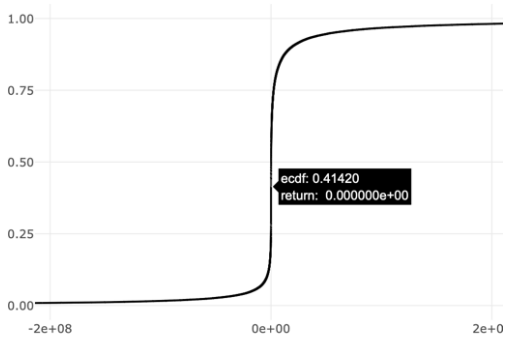
Why rational self-interest won't work

Optimizing investments at a firm level seems like it should fix the problem, but it hasn't, and I believe two concepts from economics explain why; managerial decisions and negative externalities.

What is the value of reducing risk?

50% lower likelihood of breach:

- 15% negative return >$1M
- 40% negative or zero return
- 60% positive return
- 32% positive return >$1M
- Median return $60K



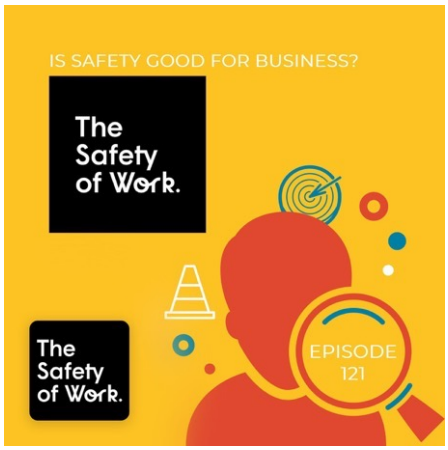
I did an analysis modeling the net present value (NPV) of risk reduction, from the perspective of a manager making an investment decision and comparing results over a 10-year period. In many cases, there is no payoff, and sometimes the payoff is negative, simply due to the high variability in outcomes. If I'm a rational manager who is rewarded for ROI, I'm going to always choose an investment with clear positive returns over something so variable, purchase insurance to cover my risk, and invest only the minimum necessary to meet security compliance.

Aside: the same analysis found a positive return for more frequent events, for example, responding to malware infections.

https://jabenninghoff.github.io/security/analysis/risk-value.html

Is ~~security~~ safety good for business?

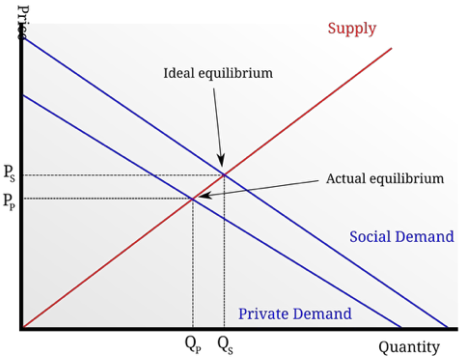
- No.
- "The Tension Between Worker Safety and Organization Survival"
- Looked at workers comp claims from 100K+ orgs
- Firms with higher injury rates were more likely to survive



I find many parallels between safety and security. I highly recommend The Safety of Work podcast, and episode 121 looks at this question for safety. "Sure, safety is expensive but imagine how much an accident will cost us!" In this episode, David and Drew review a paper that compared safety and business outcomes. That doesn't mean good safety doesn't have benefits, but good safety isn't good for the business as a whole. Sadly, I could find no similar study for cybersecurity, but I suspect it would have similar results; studies on stock price after an incident are close, which show only a short-term dip, and no difference 1+ years later.

https://safetyofwork.com/episodes/ep-121-is-safety-good-for-business
https://pure.ulster.ac.uk/ws/portalfiles/portal/78049007/The_tension_between_safety_and_survivial_final_document_jan_2020.pdf

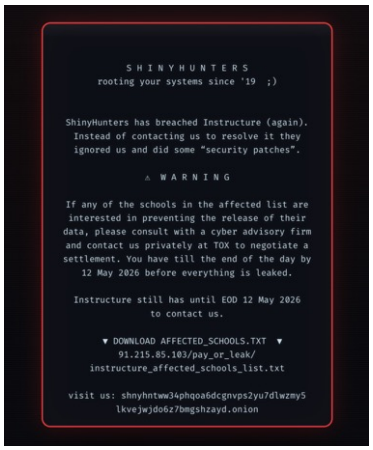
What is the cost of *not* reducing risk?

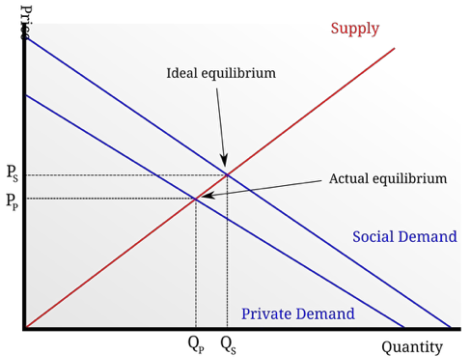


In economic theory, when the social cost exceeds the private cost of producing a good, a negative externality exists, for example, when the private cost of production doesn't account for the impact of pollution. A free market will never achieve the ideal equilibrium without regulation of some kind. Breach cost isn't just borne by the firm that was breached, but also its customers and other stakeholders. Security spending has a positive externality; the social demand for security spending exceeds the private demand, and we end up with a smaller quantity of security produced; this is similar to vaccines, which has a much larger collective benefit than individual benefit when we reach herd immunity.

https://en.wikipedia.org/wiki/Externality
Images: https://commons.wikimedia.org/wiki/File:Positive_externality.svg, https://commons.wikimedia.org/wiki/File:Usine_UNION_CARBIDE_SOUTH_CHARLESTON_KANAWHA_RIVER._from_NARA_551180.jpg

What is the cost of *not* reducing risk?





Example: Canvas/Infrastructure breach. Thousands of schools affected, many of them public institutions. The breach could cost Infrastructure (owned by KKR and Dragoneer) hundreds of millions of $, but how much additional cost will be paid by the 9000 schools affected (according to ShinyHunters)?

https://en.wikipedia.org/wiki/2026_Canvas_security_incident
https://www.404media.co/the-biggest-student-data-privacy-disaster-in-history-canvas-hack-shows-the-danger-of-centralized-edtech/
https://apnews.com/article/cyberattack-schools-canvas-instructure-shinyhunters-a0d7719689263e6b5f90d0e633391b5b
Images: https://commons.wikimedia.org/wiki/File:Positive_externality.svg, https://en.wikipedia.org/wiki/File:ShinyHunters_Hacking_Message.png

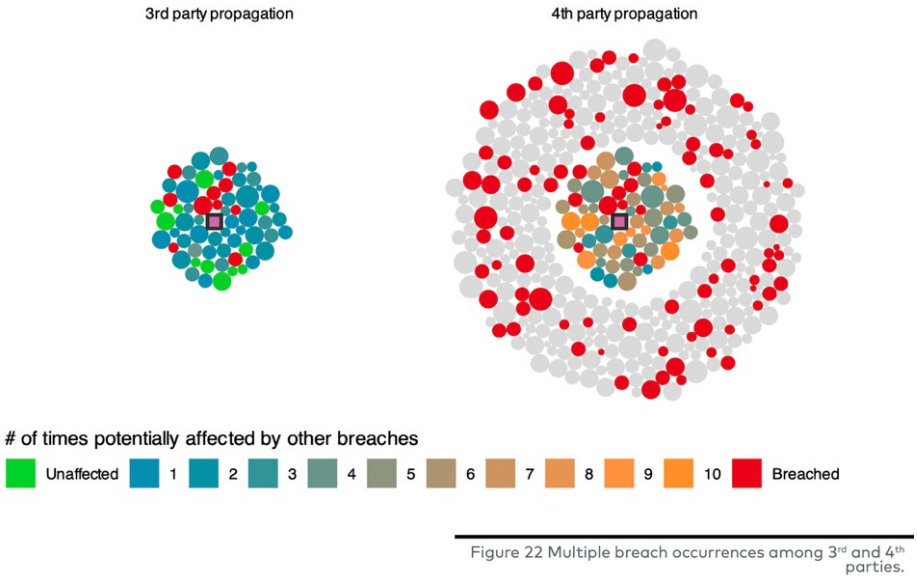
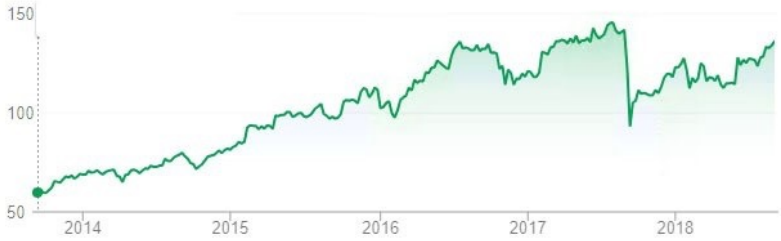


Figure 22 Multiple breach occurrences among 3rd and 4th parties.

Cyentia's research shows how 3rd party and 4th party breaches propagate, sending ripples throughout the supply chain. The optimal security investment at the breached firms doesn't account for the impact on its network. The CISO of JPMorganChase wrote an open letter on this very issue in April 2025, calling for prioritizing security and modernizing architecture. Yet simply asking won't work; the only way to solve the 3rd party risk problem is to establish minimum standards of security, and even JPMorganChase doesn't have the leverage to make this happen on its own.

RiskRecon, & Cyentia Institute. (2023). *Risk to the Nth-Party Degree: Parsing the Tangled Web*. https://www.riskrecon.com/report-risk-to-the-nth-party-degree
https://www.jpmorganchase.com/about/technology/blog/open-letter-to-our-suppliers

What about reputation?



But what about reputation impact and loss of customers? That's harder to measure, but it should affect stock price. However, multiple studies have shown that a company's stock can drop immediately following a breach, the price recovers to prior levels in a year or less. Here is a plot of Equifax's stock price, which shows this pattern.

https://www.tripwire.com/state-of-security/relation-between-breaches-and-stock-price-drops
Bischoff, P. (2024). How data breaches affect stock market share prices. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/
Image: https://portswigger.net/daily-swig/equifax-a-year-on-little-has-changed-at-least-for-the-billion-dollar-company

Solutions

Historical and Current Examples

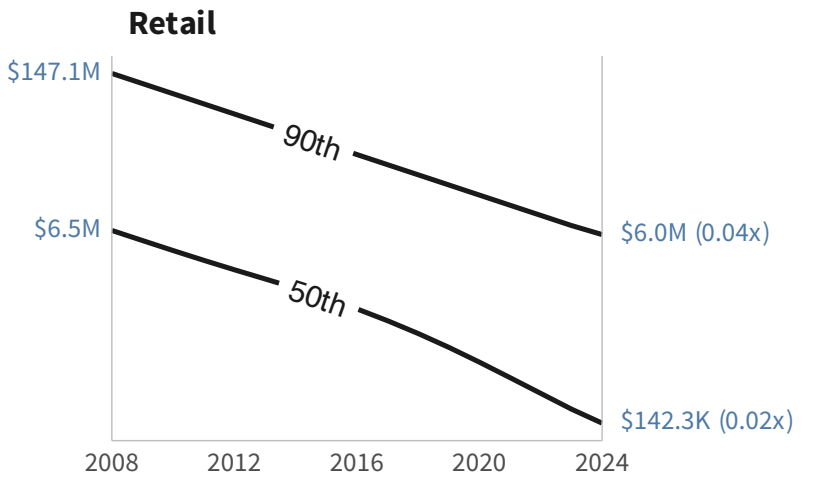
Fortunately, there are historical and current examples of solutions to this problem.

Regulation

Regulation is historically the most common solution. Auto safety is regulated by both government (NHTSA, Federal and State regulations) and insurance (IIHS); a similar combination should work well for cybersecurity, especially given the increase in cyber insurance. Underwriters Laboratories was originally funded by fire insurance companies to test electrical products for safety, and a similar organization could certify the security of software and services. The Cyber Resilience Act being implemented in the European Union introduces minimal security requirements for commercial digital products, including opt-out automatic security updates, and incident reporting. The US is starting to use the False Claims Act to regulate cybersecurity in government contracts, and companies have paid settlements to resolve claims that they misrepresented their cybersecurity posture.

https://en.wikipedia.org/wiki/National_Highway_Traffic_Safety_Administration
https://en.wikipedia.org/wiki/Insurance_Institute_for_Highway_Safety
https://en.wikipedia.org/wiki/Cyber_Resilience_Act
https://www.forbes.com/sites/emilsayegh/2026/04/01/the-false-claims-act-is-quietly-becoming-a-cybersecurity-enforcement-engine/
Images:https://commons.wikimedia.org/wiki/File:National_Highway_Traffic_Safe

ty_Administration_logo.svg
https://commons.wikimedia.org/wiki/File:CF17005-111.jpg
https://commons.wikimedia.org/wiki/File:UL_Solutions_logo.svg



Source: IRIS 2025 (Cyentia Institute Member Vault)

Losses in Retail are one of the few sectors that have seen a decline in incident costs; Cyentia speculates that this is because of PCI, I will go further and say that I think it's evidence that a prescriptive regulatory scheme that has been increasingly enforce by the card brands shows that regulation is effective at reducing security risk.

Cyentia Institute. (2025). *Information Risk Insights Study: It's About Time*. https://www.cyentia.com/iris2025/ (Fig 12)
Image: https://www.cyentia.com/membership-account/ (IRIS 2025 Report Figures)

Liability

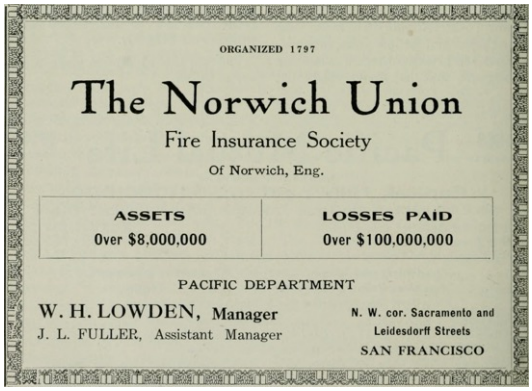
Legal liability is an indirect form of regulation; consumer product safety, including warning labels and product recalls, is largely driven by manufacturers wanting to protect themselves against lawsuits. We could change laws around software and software licensing to shift greater liability to tech companies.

https://www.routledge.com/Handbook-of-Warnings/Wogalter/p/book/9780805847246
Image:
https://commons.wikimedia.org/wiki/File:16_CFR_§_1205.6_Warning_label_for_reel-type_and_rotary_power_mowers.svg

Insurance

- Type of data (PHI, SSN)
- Number of records
- Gross revenue

- Use of MFA
- Use of EDR
- Secure email gateway
- Phishing training
- Backups

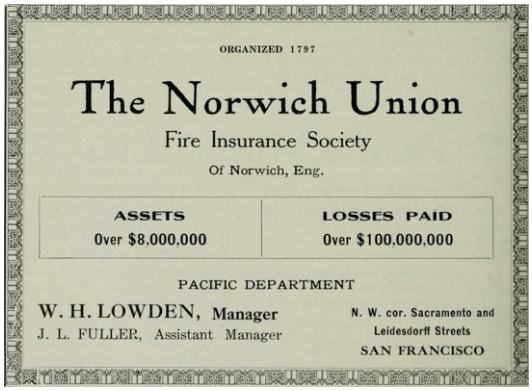


A cyber insurance broker shared an application form with me, and insurers are starting to ask questions about security practices – if an org has PHI, more than 100K sensitive numbers (excluding employees), or more than $25M in gross revenue, then the security specific questions must be answered, which include MFA, EDR, secure email (anti-phishing), phishing training, and backups. This is a good start, but I haven't seen the same kind of prescriptive regulation like we see in PCI-DSS. I'm happy to see from previous talks that the insurance industry is working on this, and I'd like to see more, including an IIHS-like organization - the "Insurance Institute for Cybersecurity (IIC)". TPRM could help accelerate this by requiring specific coverage levels for vendors and partners.

https://content.naic.org/sites/default/files/cmte-h-cyber-wg-2024-cyber-ins-report.pdf
Image:
https://commons.wikimedia.org/wiki/File:Coast_review_(1910)_(14760820941).jpg

What Works in Cybersecurity

1. Ditch the perimeter appliance (VPN, Firewall)
2. Patching: replace CVSS with KEV + EPSS
3. Phishing Resistant MFA
4. Avoid running your own infrastructure – use Cloud!



Daniel Woods has been working on the "what works in cybersecurity" question, and has used claims data and published research to answer the question. His current top 4 recommendations include the following (with some of my own modifications). 1. Deperimeterize 2. Patch KEVs ASAP. 3. Enforce MFA on email, remote access, audit MFA enforcement. 4. Use Cloud, especially Google Workspace.

https://www.linkedin.com/posts/are-you-investing-in-the-right-cybersecurity-ugcPost-7440680207281364992-5b8M/
Image:
https://commons.wikimedia.org/wiki/File:Coast_review_(1910)_(14760820941).jpg

Professionalization

There's another way of regulating security, one that can be implemented within organizations, what I call the "professionalization" of technology engineers (infrastructure and software). I like to explain this by way of a terrible accident – in 1981, two walkways in the Hyatt Regency hotel in Kansas City collapsed into the lobby below, killing 114 people and injuring over 200. The head engineer accepted full responsibility for the accident, and it led to engineering safety reforms. By accepting responsibility and making the engineer personally accountable for safety, it gave future engineers moral standing to push back against employers who ask them to do something unsafe, and the backing of law and professional licensing organizations. We don't yet have this in technology, and while there are downsides to licensing, I think the benefits now outweigh the costs.

https://en.wikipedia.org/wiki/Hyatt_Regency_walkway_collapse
Images:
https://commons.wikimedia.org/wiki/File:Hyatt_Kansas_City_Collapse.gif
https://commons.wikimedia.org/wiki/File:Hyatt_Regency_collapse_floor_view.PNG

Professionalization

The IEEE is working towards a Software Engineering Certification and has published SWEBOK v4, which includes a chapter on Security!
ISC2 recently launched the Code of Professional Conduct, which includes a commitment to stakeholders, including clients and third parties. Code of Conduct Task Force is working on further development and promotion of the Code. Hillel Wayne also explored the question “Are We Really Engineers?” by interviewing 17 people who had worked as both a traditional and software engineer and concluded: YES! - he presented this at SRECON EMEA 2024. By making our front-line engineers responsible for security, it changes our role, from governance to support – helping our engineers succeed.

https://www.computer.org/education/certifications
https://www.isc2.org/Insights/2026/02/ISC2-launches-Code-of-Professional-Conduct-to-elevate-cybersecurity-practices
https://www.usenix.org/conference/srecon24emea/presentation/wayne
https://www.hillelwayne.com/post/are-we-really-engineers/
Images: https://commons.wikimedia.org/wiki/File:IEEE_logo.svg, https://commons.wikimedia.org/wiki/File:ISC2_Logo.svg

Social Change

The hard truth – we likely won't see change until a major incident creates sufficient outrage and a social movement for change. This is what happened with auto safety, when Unsafe at Any Speed became a surprise best seller, and led directly to congressional hearings and the creation of the US Department of Transportation and the National Highway Traffic Safety Administration.

https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed%3A_The_Designed-In_Dangers_of_the_American_Automobile

Call to Action

- Educate and advocate
- Insurance premiums
- Professionalize technology and security engineering

1. Educate and advocate on the need for change; call for online services to *offer* Passkey based authentication; this is a bit like requiring auto manufacturers to install seat belts in all cars.
2. If you're insurance, work to support what works in security through premiums.
3. For all of us, within our organizations and professional associations, work to make technology and security engineering a professional practice.

Image: https://en.wikipedia.org/wiki/File:I_Want_You_for_U.S._Army_by_James_Montgomery_Flagg.jpg

Thank you!

Thank you!

Slides, Connect & Resources

Resources:
cyentia.com
cisa.gov
isc2.org

Connect:
linkedin.com/in/jbenninghoff/

Website:
jbenninghoff.com
security-differently.com

Scan the QR code for slides and more! Questions?