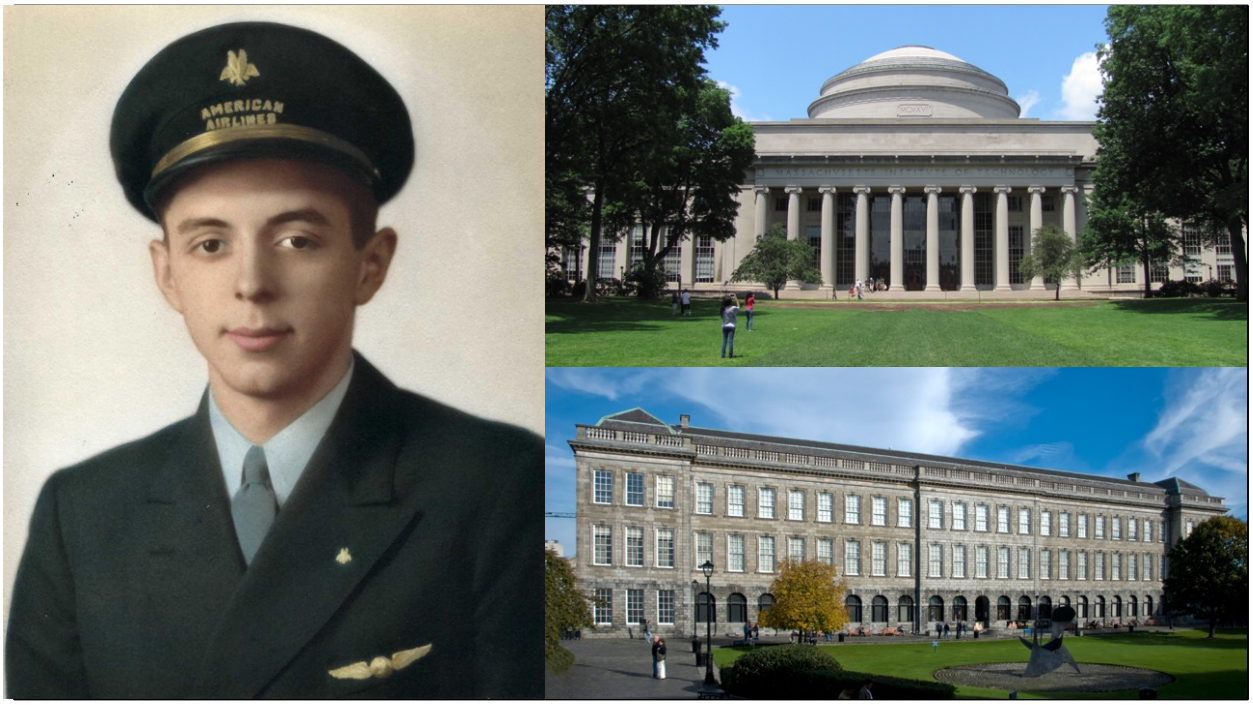
Security Differently

John Benninghoff

Hi, I'm John Benninghoff and this is a story about looking at security through a different lens. This is a short presentation, so I encourage you to make it more interactive by asking questions throughout. I'll have a QR code at the end for you to download the slides with notes and links to all the references.

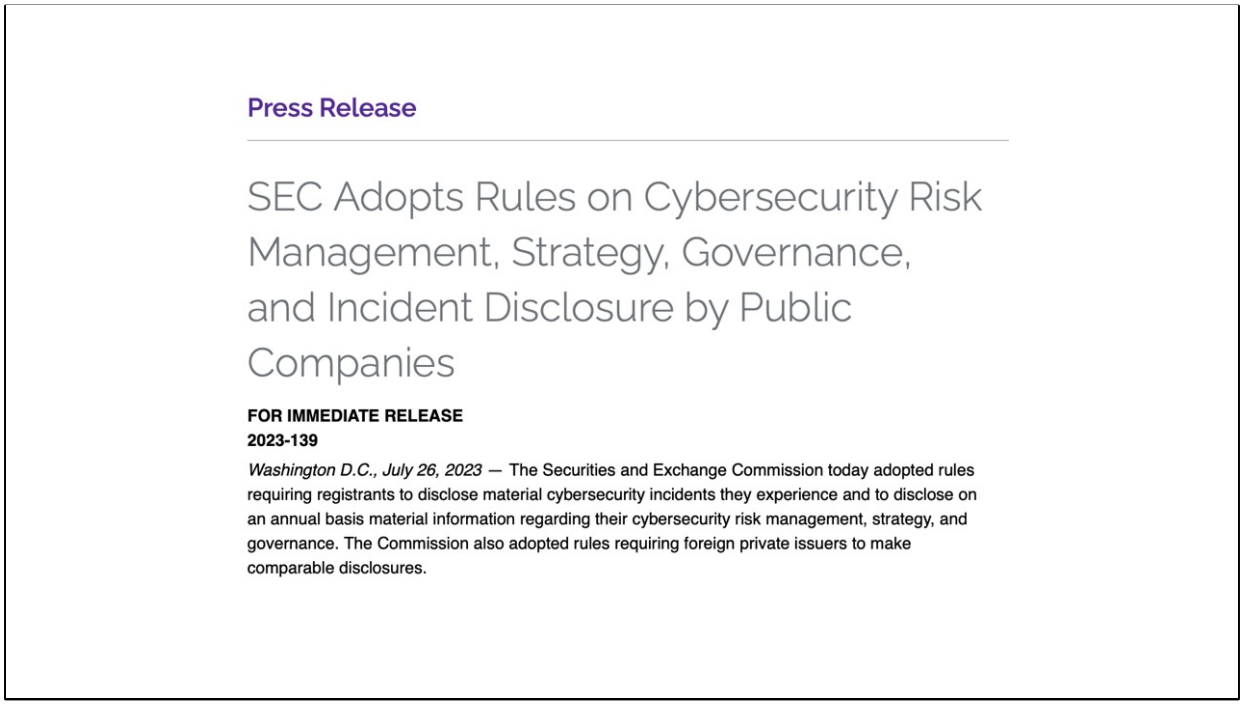


”About Me”
My grandfather: the pilot of ~65 years (15-80), circa 1940, always used his pre-flight checklist, started my interest in aviation safety, *The Checklist Manifesto*. I asked, “Can we use this for security?”
This led me to the book Engineering a Safer World by Nancy Leveson, the “new view” of safety, and the STAMP/STPA Workshop @ MIT.
Later, I started a Masters degree at Trinity College Dublin, studying safety science and how we can apply it to security and reliability.

https://psas.scripts.mit.edu/home/
https://www.tcd.ie/courses/postgraduate/courses/managing-risk-and-system-change-msconline/

Security is Increasingly a Priority…

(pause)



Press Release

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE
2023-139

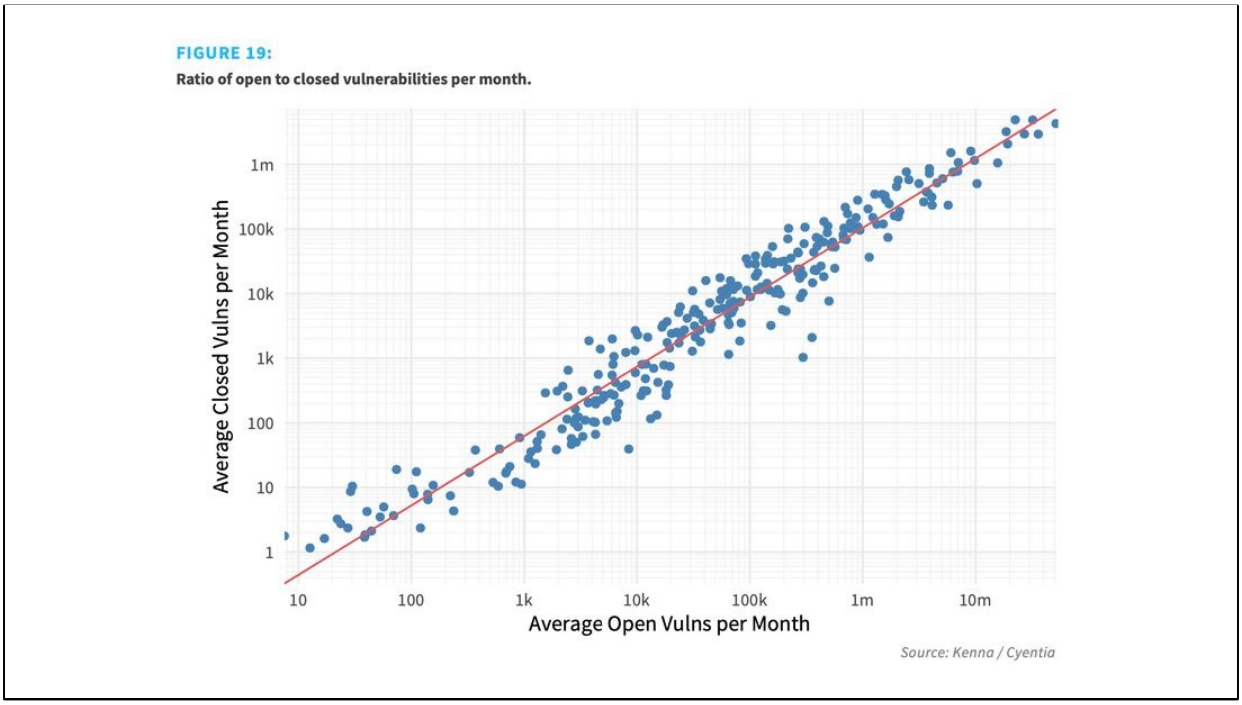
Washington D.C., July 26, 2023 — The Securities and Exchange Commission today adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures.

Security is increasingly a priority – the latest SEC rules on Cybersecurity is a prominent example. The new rules are both an acknowledgement of the increasing importance of managing security effectively, and an incentive for publicly traded companies to prioritize security. Other evidence - in a recent report, Cyentia and RiskRecon found that 90% of survey respondents reported that third party risk management was a growing priority in 2023.

https://www.sec.gov/news/press-release/2023-139
https://www.riskrecon.com/state-of-third-party-risk-management-2024

…yet security outcomes aren’t changing

(read)



We've had Vulnerability Management since 2001-2002, and yet we still struggle.

In 2019, Cyentia and Kenna found that "A typical organization will have the capacity to remediate about one out of every 10 vulnerabilities in their environment within a given month. That seems to hold true for firms large, small, and anywhere in between." – there are no economies of scale, and the number of open vulns is growing over time.

https://www.cyentia.com/the-hidden-complexity-of-vulnerability-remediation/
2002 papers on VM:
https://doi.org/10.1016/S1353-4858(02)05013-4
https://doi.org/10.1016/S1363-4127(02)00104-8

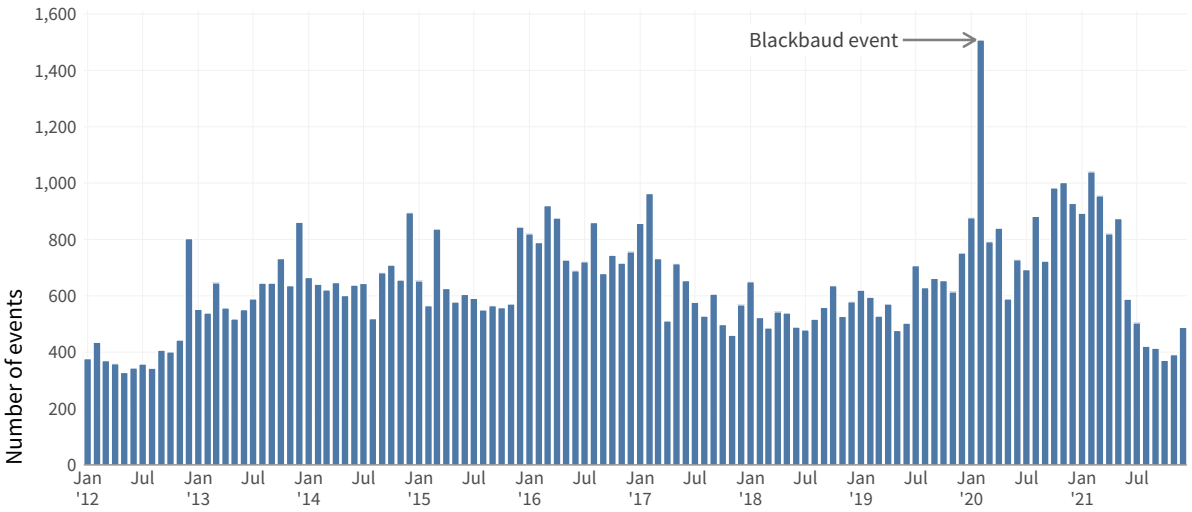


Figure 1: Number of publicly reported cyber loss events each month from 2012 to 2021

What about breaches?

This chart from Cyentia's IRIS (Information Risk Insights Study) 2022 report shows that the number of publicly reported cyberattacks has stayed largely the same over the past 10 years.

https://www.cyentia.com/iris-2022/

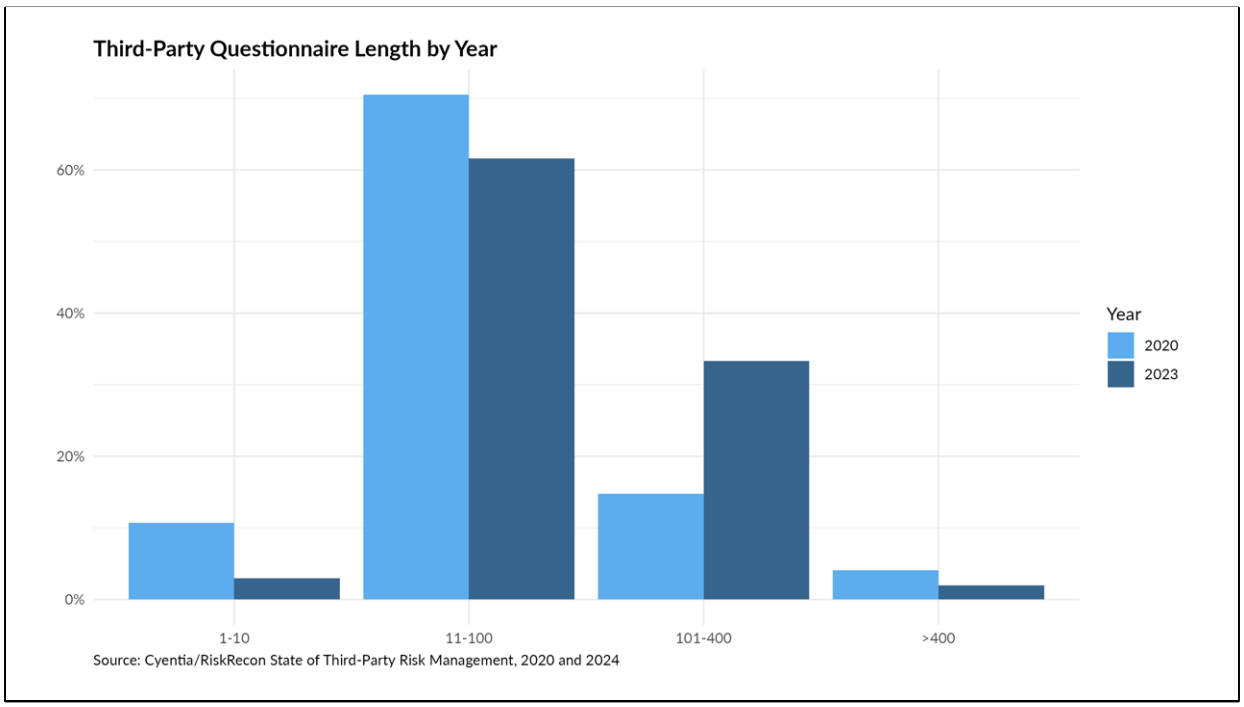
Probability of a firm experiencing a given number of events			
Revenue category	One or more	Two or more	Three or more
Upper Bound			
More than $100B	29.33%	9.32%	3.56%
$10B to $100B	21.93%	4.91%	1.28%
$1B to $10B	17.04%	3.09%	0.71%
$100M to $1B	12.95%	1.56%	0.23%
$10M to $100M	11.53%	1.12%	0.11%
Lower Bound			
More than $100B	29.30%	9.31%	3.49%
$10B to $100B	14.20%	2.73%	0.71%
$1B to $10B	6.56%	0.88%	0.22%
$100M to $1B	2.18%	0.14%	0.02%
$10M to $100M	0.46%	0.02%	0.00%

Table 2: Quick reference for loss event frequency estimates

How likely is a breach?

The largest firms, over $100B in revenue, have about a 30% chance of experiencing one or more loss events in the next 12 months. Smaller orgs are less likely to experience a breach, but the impact can be larger as a proportion of annual revenue.

https://www.cyentia.com/iris-2022/



Policies, Procedures, and Controls also grow over time; some organizations have accumulated over 20 years of rules. An example of this: third-party questionnaire length, as reported by Cyentia and RiskRecon. The number of organizations with 101-400 questions more than doubled between 2020 and 2023, at the expense of shorter questionnaires. (And the effectiveness of the questionnaires is, questionable)

2020 data: https://www.riskrecon.com/state-of-third-party-risk-management-report
2023 data: https://www.riskrecon.com/state-of-third-party-risk-management-2024

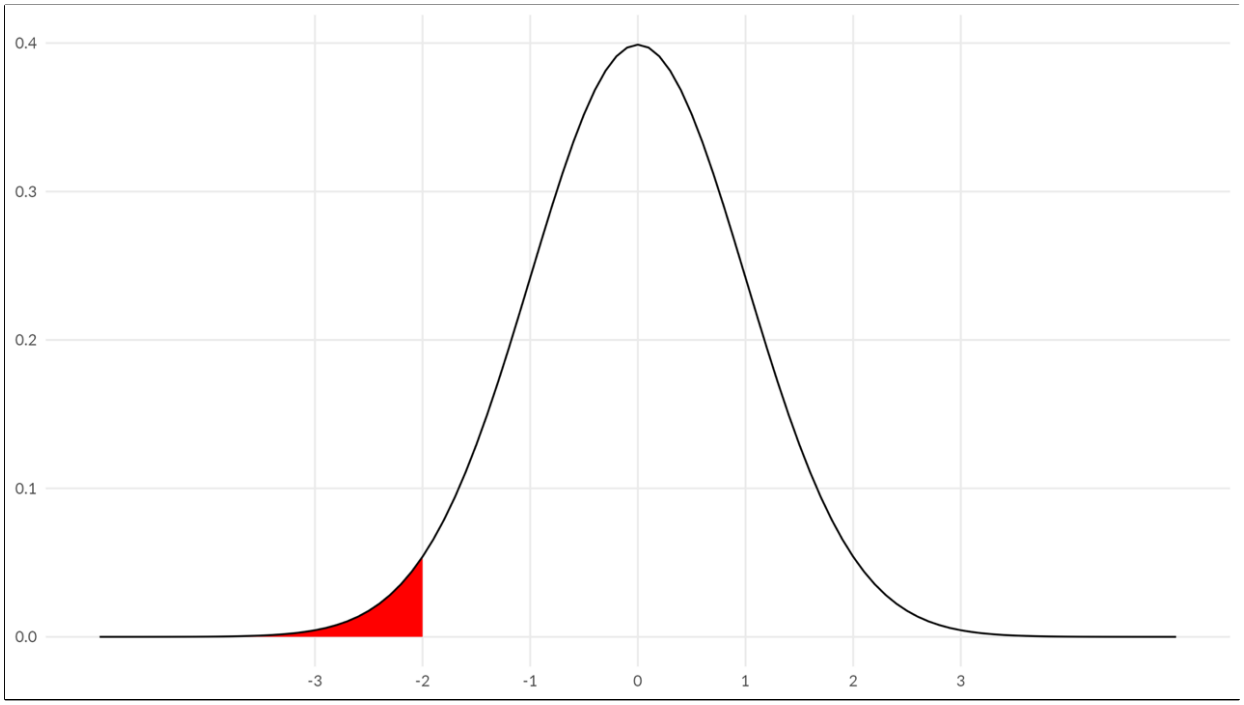
The “New View” of Safety

Safety-II and Safety Differently

If security outcomes aren’t improving despite the increase in priority, what do we do? Safety faced the same problem years ago, and the “New View” offers an answer.

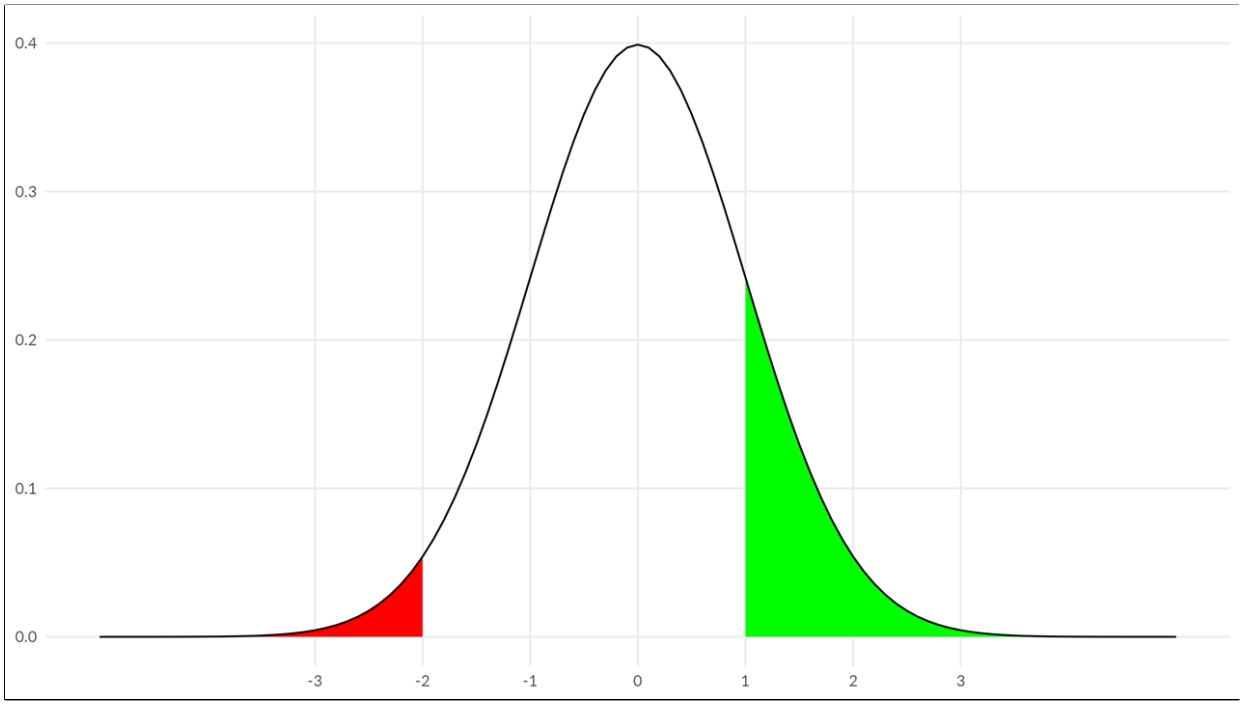
Erik Hollnagel, the scientist who created “Safety-II”.

https://erikhollnagel.com



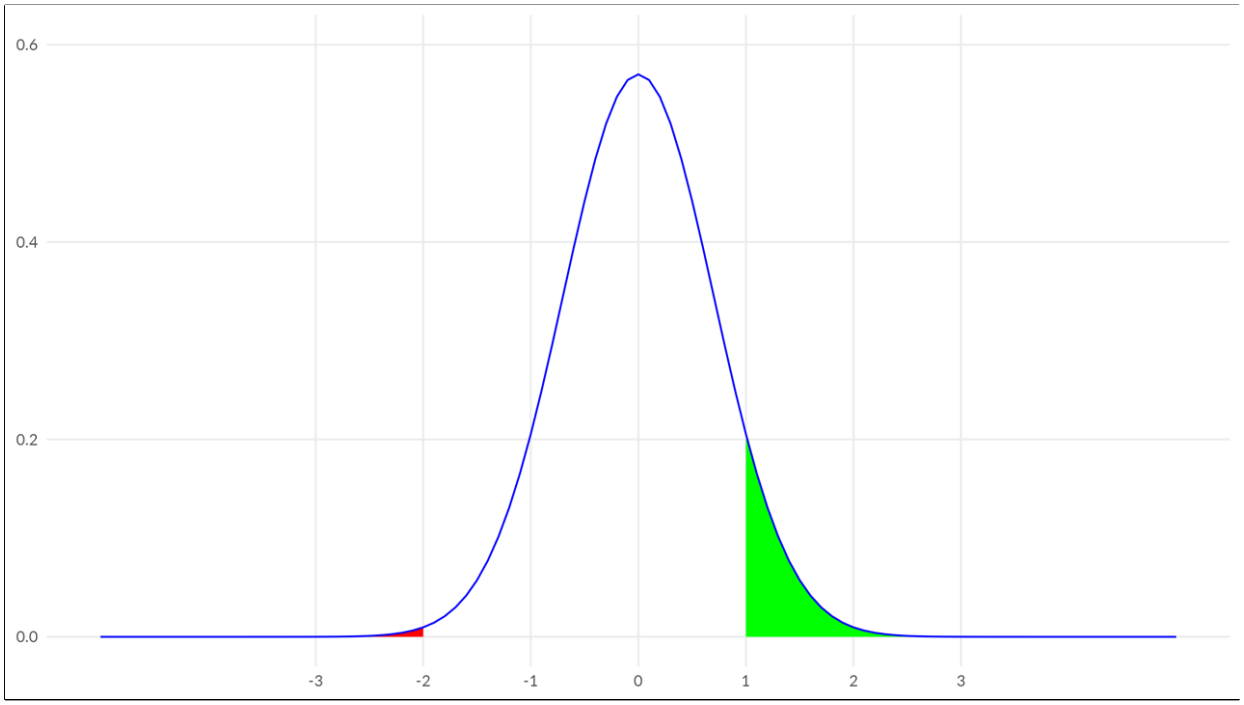
Hollnagel observed that in safety, much like security, we tend to focus on only the bad outcomes. Success happens when we avoid the bad outcomes, shown on this normal curve in red.

R source code for visualizations:
https://jabenninghoff.github.io/rtraining/analysis/constraints.html

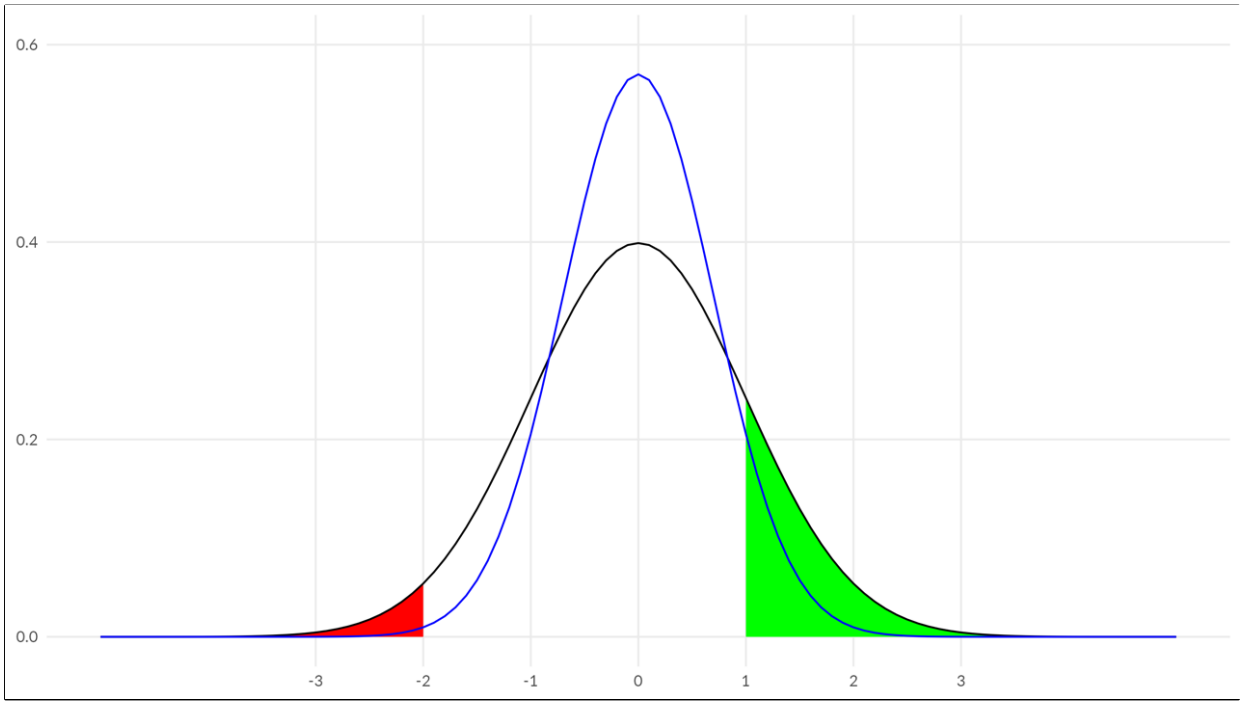


He argued that we can't have a science based on the non-occurrence of bad events – you can't study something that doesn't happen – instead, we must consider and study the whole range of outcomes, including good (green) and bad outcomes, and the "normal" outcomes between.

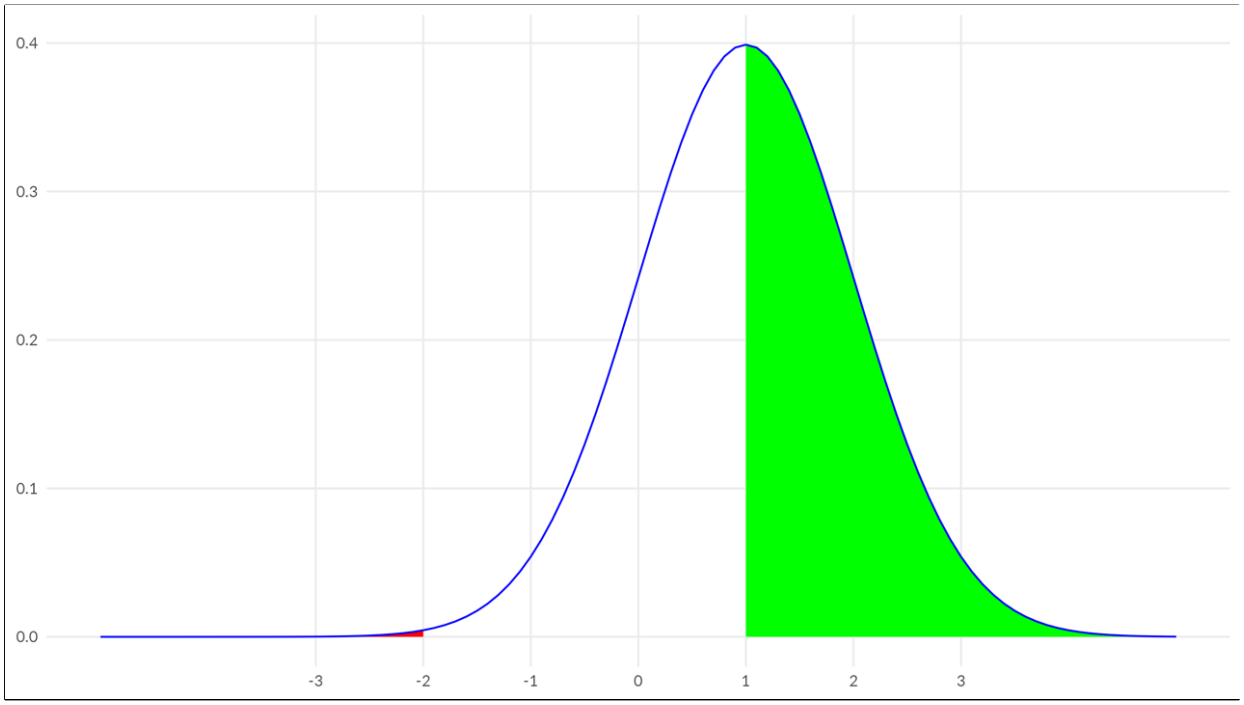
I've observed that there are two ways of reducing bad outcomes.



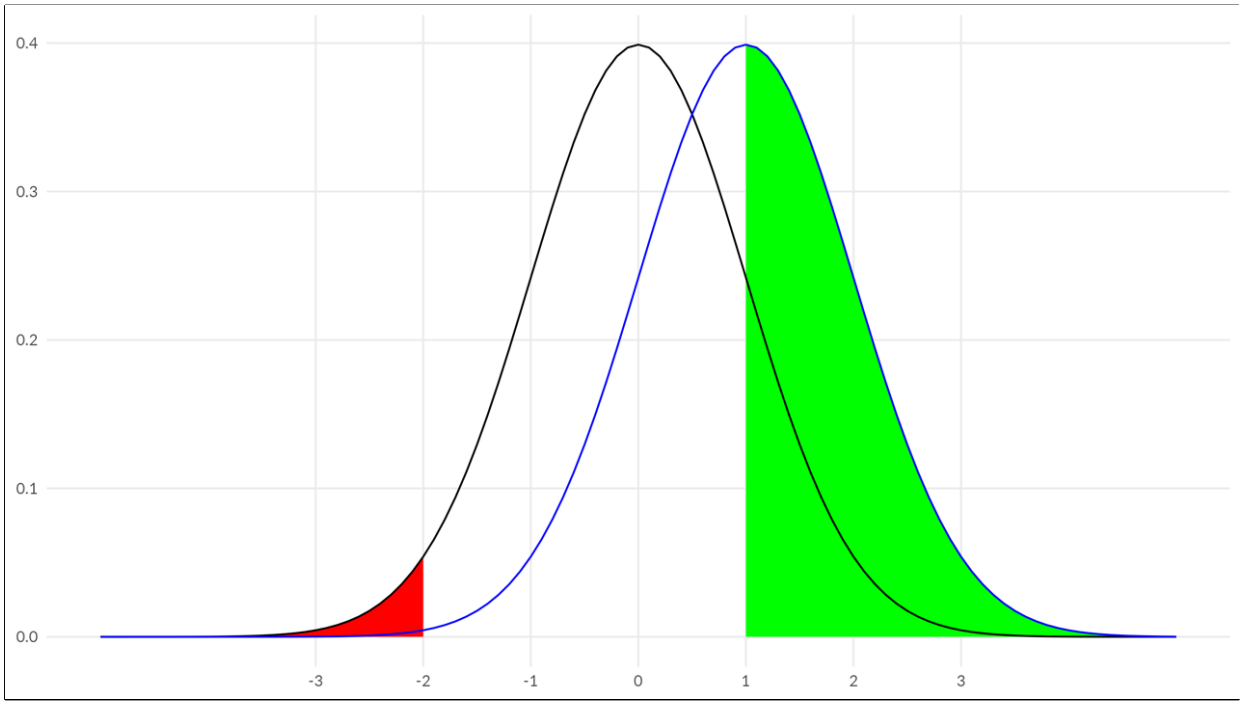
One way is to constrain behavior – introducing policies, controls and procedures that protect against negative outcomes – making the curve narrower.



However, constraints reduce both unexpected negative *and* positive outcomes, shown here. This shows the downside of controls. (effect of change management on DevOps performance)

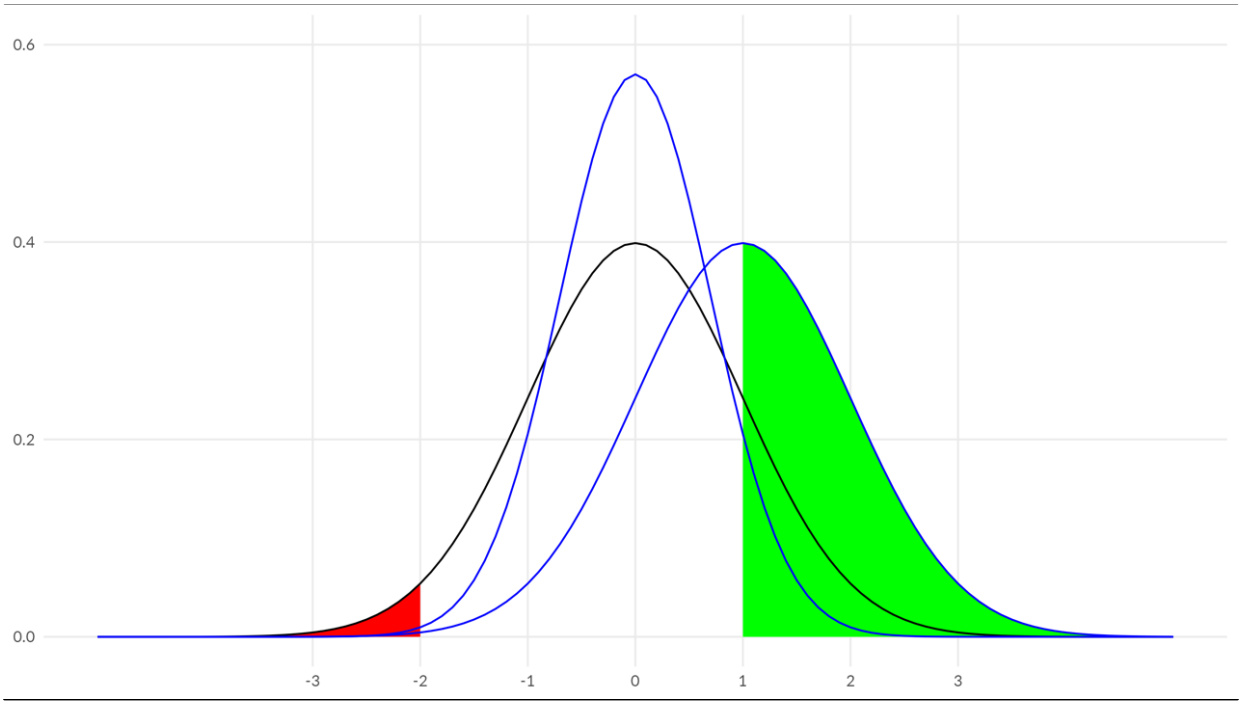


Another, better, way to reduce bad outcomes is by improving performance – shifting the curve to the right.



Focusing on improving performance means that security is no longer an expense, since it both reduces bad outcomes and increases good outcomes. (DORA research)

https://dora.dev/research/



Bringing all three together, this model shows how improving performance is a better strategy – which raises the question, how do we improve security performance?

Part of this is perspective: "I have good security because my home network has never been breached by the Russian or Chinese Governments" vs "We have good security because we successfully defended against an internal red team attack" - preventing occurrence vs performing when exposed to threats.

Sidney Dekker, a safety scientist and commercial pilot, who created Safety Differently. A documentary published in 2017 showcases how three organizations in Australia adopted Safety Differently; examples from the movie showcase how SD can be adapted to Security.

https://sidneydekker.com

Scene from ”Safety Differently - The Movie”. This is a key intersection in the town of Drachten, which used to have the usual traffic controls: lights, signs, barriers, etc. The problem? 10 serious accidents a year, and congestion at busy times. The traffic engineers removed all the controls, forcing cars, bicycles, and pedestrians to figure out how to safely navigate the square. This resulted in a *reduction* in accidents from 10/year to 1/year and eliminated congestion. A “riskier” environment created greater safety!

Safety Differently - The Movie: https://www.youtube.com/watch?v=EeIucLnEa24 and https://vimeo.com/821575893
https://sidneydekker.com/safety-differently-movie/ (2017)

Traditional Safety	Safety Differently
• Workers and mistakes are the cause of poor performance	• People aren't the problem, they are the solution
• Organizations create Controls, Policies, and Procedures to prevent mistakes and regulate worker behavior	• Support workers by providing the tools and environments to work safely
• Success is measured by the absence of negative events	• Safety is measured by the presence of positive capacities

Dekker's Safety Differently advocates for intervening in work conditions instead of trying to control behavior ("Human Error is the cause of all our troubles"); create an environment, like the intersection in Drachten, that promotes safety. [Review Traditional Safety vs Safety Differently]. Shift emphasis from compliance and paperwork to successful operations. This isn't easy – you're giving up control, or rather, the illusion of control.

Further reading: https://www.information-safety.org/2023/10/31/security-differently/

Safety Differently – The Movie

- Group 1:
  - No changes (control)
- Group 2:
  - No national procedures, full autonomy, clearances sought from industry regulator
- Group 3:
  - Full autonomy, staff trained in leadership and Safety Differently methods

Woolworth's, a grocery chain in Australia. Safety at stores is an important issue, for both staff and customers (slip-and-fall). Had traditional centralized, national safety rules and procedures. Executives asked the question, "what if we remove all the safety rules for the stores, like the intersection in Drachten?" Which led to an experiment:

Group 3 had the best results: lowest incidents, best ownership and engagement, local control, strongest leadership. Non-managers corrected each other.

Security is not Safety! How do we make Safety Differently work for us?

Incentives are different for security, as the front-line workers are further removed from risk than in most safety contexts. For the most part, the technology staff that create security aren't directly impacted by negative events, the organization is. Even within the world of safety, best practices from one industry (aviation) don't transfer directly to another (marine safety).

For more on this topic, see: https://www.information-safety.org/2024/04/09/sre-isnt-safety/

The Movie – Program on a Sticker

Safety

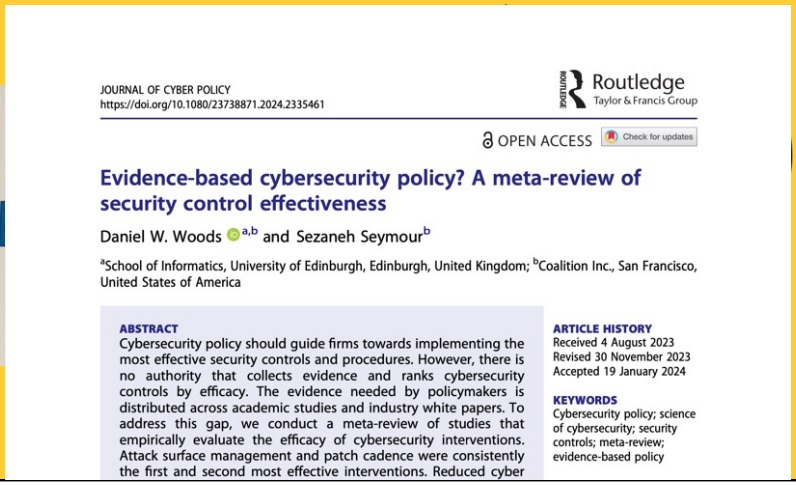
Security

Origin Energy (an Oil & Gas company) saw safety getting worse over time. The work of safety was disconnected from the safety of work, with the safety officer in the office 60-70% of the time, and a safety plan created “in the boardroom”. Using safety data, the new approach was to focus in on what mattered and replaced the 30-page safety plan that sat in a drawer with a STICKER that could be used in all operations. But what would a security program sticker look like?

Safety Differently - The Movie: https://www.youtube.com/watch?v=EeIucLnEa24 and https://vimeo.com/821575893
https://commons.wikimedia.org/wiki/File:Question_mark_(black).svg

The Movie – Program on a Sticker

Safety



JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2024.2335461

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Evidence-based cybersecurity policy? A meta-review of security control effectiveness

Daniel W. Woods [a,b] and Sezaneh Seymour[b]

[a]School of Informatics, University of Edinburgh, Edinburgh, United Kingdom; [b]Coalition Inc., San Francisco, United States of America

ABSTRACT
Cybersecurity policy should guide firms towards implementing the most effective security controls and procedures. However, there is no authority that collects evidence and ranks cybersecurity controls by efficacy. The evidence needed by policymakers is distributed across academic studies and industry white papers. To address this gap, we conduct a meta-review of studies that empirically evaluate the efficacy of cybersecurity interventions. Attack surface management and patch cadence were consistently the first and second most effective interventions. Reduced cyber

ARTICLE HISTORY
Received 4 August 2023
Revised 30 November 2023
Accepted 19 January 2024

KEYWORDS
Cybersecurity policy; science of cybersecurity; security controls; meta-review; evidence-based policy

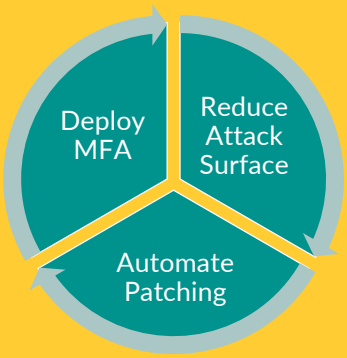
A recently published paper suggests an answer – the three most effective ways of improving security are: 1. reducing attack surface, 2. patching faster, and 3. *fully* implementing MFA. Note: these are measures of organizational effectiveness, driven primarily by operations, infrastructure and development, not security.

Paper: https://doi.org/10.1080/23738871.2024.2335461

The Movie – Program on a Sticker

Safety

Security



So, a security program on a sticker might look like this…

The Movie – Program on a Sticker

Safety

Security

Or even focus in further in the current year on the biggest challenge… and, if patching is fully automated, the only security function is identifying when the automation is broken.

The Movie – Roles and Responsibilities

Safety

- CEO takes responsibility for Safety
- Operations owns Safety
- Safety metrics measure positive outcomes, not absence of negative outcomes

Security

- CEO takes responsibility for Security
- Operations/Infrastructure and Development own Security
- Security metrics measure positive outcomes, not absence of negative outcomes

The CEO of Origin says it well: “The first thing you need to do as a leader of your business is take accountability for the performance of your business. [including safety] … it’s not the safety team’s problem to solve … it’s my problem to solve. [leveraging the skills of the people around you for solutions]” It also means shifting ownership of security to those who create it; in technology that’s both operations and development. We need to adopt security metrics that focus on success, like work that promotes security (patching) and how well the organization does when exposed to threats.

“We don’t ask the CFO to make the company profitable, but we do ask the CISO to make the company secure.”

- Chris Brown

I spoke to a colleague about the role of the CISO and how it should function more like the CFO, and he told me this.

This quote should bother you. Like the CFO, the CISO has an important role to play, but security, like safety and profitability, is a shared responsibility. For cybersecurity, this means the CISO becomes more like the CFO, keeping score with metrics (the security budget), setting strategy, and supporting business units to meet their security budget.

More on this topic: https://www.information-safety.org/2024/02/20/security-as-finance/
Chris: https://www.linkedin.com/in/chrisbrownforhire/

The Movie – Department Size

Safety

Security

The head of safety at Origin cut the size of the team from 20-30 people down to 5, an 80% reduction. “I needed to do that because we actually needed to step out of managing safety performance, and while we were in there doing their job, it created no space for them to do their own job.”

Security: maybe not a full 80% reduction; the shift in responsibilities could very well address the cybersecurity labor shortage. What’s important here is not the reduction in the size of the security team, but the shift in mindset that led to the reduction.

The Movie – Ask, Don't Tell

Safety

- Visit healthcare workers at their workplace
- Ask them what they want to learn
- Focus on learning, not compliance

Security

- Observe how staff do their jobs (technology and others)
- Ask them what they want to learn
- Focus on learning, not compliance

Metro North Hospital (Queensland Health Service) – shifted from centralized training program in Brisbane to visiting the local hospitals and clinics and asking the healthcare workers what they wanted to learn at their workplace. Learning, not compliance. "You're here to do what? You're going to ask us what we want?" Don't tell us how to do our jobs, help us learn.

The Movie – Ask, Don't Tell

Safety

- Visit healthcare workers at their workplace
- Ask them what they want to learn
- Focus on learning, not compliance

Security

Security Example: Marcus Ranum, while working on securing a Hollywood company, discovered a group of people that had a very high rate of opening malware. So, Marcus went to meet the people in the department and simply asked what they were doing – their job was to open and read ALL the email attachments. So, he asked "could you do it on an iPad?" YES!

https://commons.wikimedia.org/wiki/File:Mjr-portrait-picture-mid.jpg

The Movie – Safety Clutter

Safety **Security**

From the second movie, “Doing Safety Differently”. It’s helpful here to define Safety Clutter.

https://www.youtube.com/watch?v=eqwBA4nj5CY and
https://vimeo.com/827919411

Safety Clutter: Definition

- Accumulation of policies, procedures, and controls that don't contribute to safety
- Possibly was useful once, but isn't now, and we still do it
- It's much easier to add rules than remove them

Does this sound familiar?

Safety Clutter: https://safetyofwork.com/episodes/ep80-what-is-safety-clutter

The Movie – Decluttering

Safety
- What's working, what isn't?
- Identify sources of friction
- Does it help safety?

Security
- What's working, what isn't?
- Identify sources of friction
- Does it help security?

Safety Differently case study at Queensland Urban Utilities (water & sanitation). Kym Bancroft joined the company as HSE (Health, Safety and Environment) leader. First looked at what was working, what wasn't - identify sources of friction. "It's so easy to add to your safety management system" - decluttering, "Does it help the worker?"

The Movie – Decluttering

Safety

- What's working, what isn't?
- Identify sources of friction
- Does it help safety?

Security

Security Example: at a past company, some of us started noticing a strange issue: one day, we could no longer install a development tool binary using homebrew, but we could install it from source (it would fail at 99%). This bothered me so I started looking into it. Eventually I found that our proxy had a security rule to block Flash, Silverlight, and Java Applets. In an older version of the proxy, this only blocked direct downloads of .jar files, but the new version also looked inside archives and blocked those too. A security rule designed to block plugins that were no longer supported by any possible web browser was preventing us from installing development tools. Eventually, I was able to get this security rule removed, but only through persistence as there was no process for removing a security rule, only adding…

Support for Flash, Silverlight, and Java Applets: https://en.wikipedia.org/wiki/NPAPI, https://en.wikipedia.org/wiki/Java_applet
https://commons.wikimedia.org/wiki/File:ProhibitionSign2.svg

Security Differently

- CEO owns security, sets security goals
- CISO sets strategy and measures performance against the goals
- Security provides expertise and support to achieve the goals
- Security is an investment in improved performance, not a cost

What would an organization doing security differently look like?

By investing in things go well, they won't go wrong, and productivity, efficiency, and quality will improve as well.

It’s easier to study when things go right because it happens all the time.

- Erik Hollnagel

Practical Takeaways

Fully adopting Security Differently requires leadership buy-in

- Start by removing Security Clutter
- Seek to understand how work is done
- Focus on what's most important

So – how can you get started? Fully requires "flipping the script". Doing so is hard as we have to escape the "shield mentality," that we need to protect people from mistakes, and requires leadership buy-in. You can start by removing clutter, learn how work is done, and focus on what's most important.

Hat tip to safetyofwork.com podcast's practical takeaways!

Slides, Connect & Resources

Connect:
linkedin.com/in/jbenninghoff/

Website:
information-safety.org

Resources:
cyentia.com
erikhollnagel.com
sidneydekker.com
safetyofwork.com

Scan the QR code for slides and more!