BREACHRX

Incident Response – Why We Need a Legal Playbook

Andy Lunsford

March 14, 2025

Our Team

Founding Team

Proven track record with decades of experience in cybersecurity, data privacy, compliance, engineering & product development, and large-scale commercial litigation.

ANDY LUNSFORD
Chief Executive Officer & Founder

Privacy Expert & Attorney,
20+ years

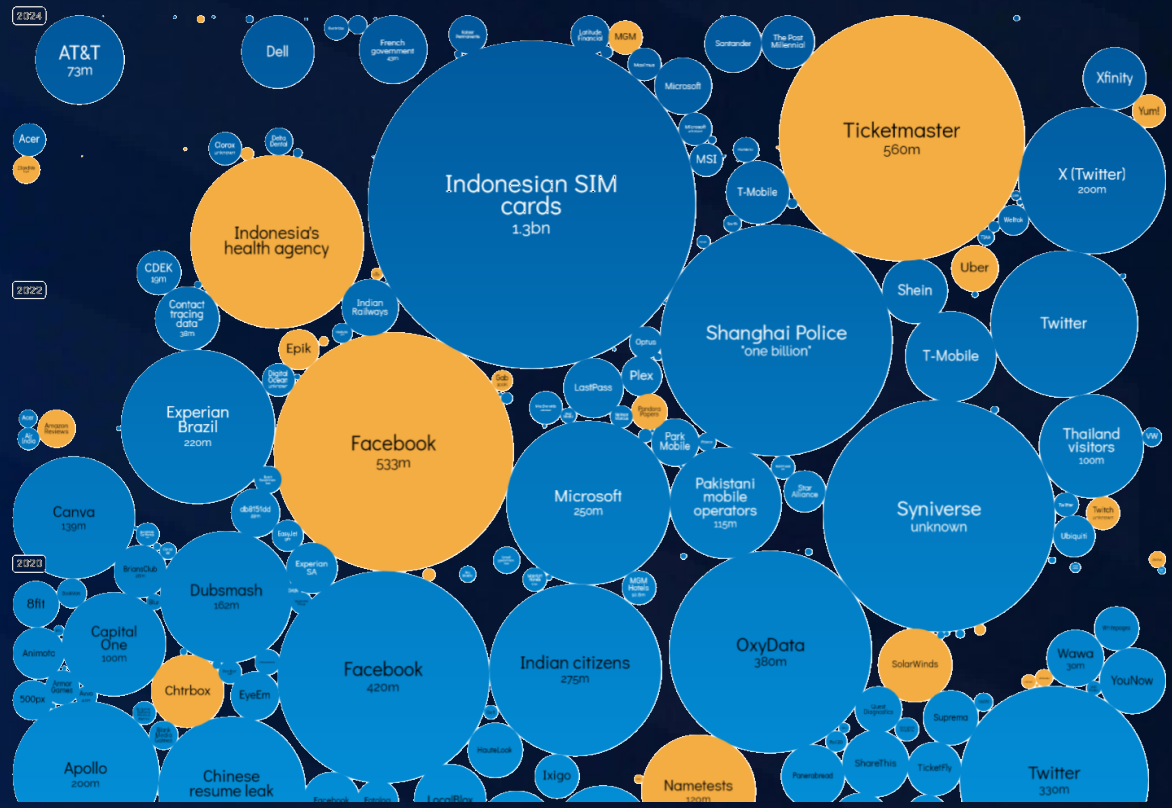
Walmart
BEACON GROUP LLC
Wharton University of Pennsylvania

MATT HARTLEY
Chief Product Officer & Founder

Cybersecurity Expert,
25+ years

FIREEYE
MANDIANT
iSIGHTPARTNERS
U.S. AIR FORCE
LOCKHEED MARTIN
Rensselaer

Has anyone here not had their data stolen?



Source: informationisbeautiful.net - last updated Jun 2024

Not so fun data breach facts

Still nation-states and criminals, increasingly third parties & insiders

Healthcare, Financials, not just Government, are highly targeted

US, Middle East in the crosshairs

Mean time to identify: 194 days
- To contain: another 64 days
- This is a 7-year low

Another report has 10 days for mean time to identify in the US

626 new malware families in 2023

10K breaches reported last year
- 32% with ransomware elements
- 10% with theft of data, extortion
- 46% involve customer personal information

Number of incidents in 2023: 2,814.
Number of breached records: 8,214,886,660

54% of companies learned about a breach from external sources

Breaches cost $4.88M on average
- In the United States, $9.36M
- Increasing about 10% YoY
- Only 2100 to 113,000 records impacted

Mega-breaches of 50-60M records: $375M

+11% YoY in lost business & post-breach response costs

Ransomware payments surpassed $1B in 2023

Cybercrime costs exceed $1T globally by some accounts (or will soon, by others)

Sources: Cost of a Data Breach report, Verizon DBIR, others, 2023-2024

Incidents Happen

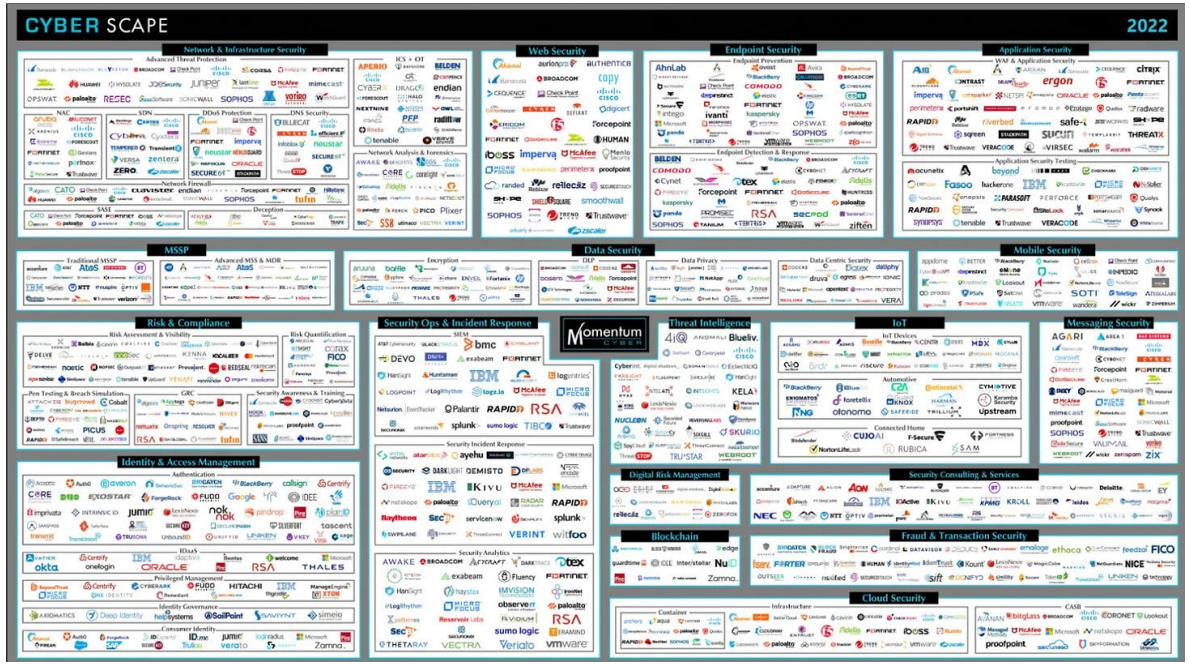
Are we prepared?

The current best practice in Incident Response

- Cybersecurity technology & expertise
- Incident response plan
- Annual tabletop exercises
- Experts on retainer
- Don’t write anything down
- Cyber insurance

Are these effective?

Is cybersecurity technology working?



5000+ cybersecurity companies
47 different cybersecurity solutions on average per organization
53% of experts admit they don't know how they work

The industry is oriented to fully automated technologies saving the day
We do have a talent gap of ~3-4M with estimates up to 85M by 2030
And yet…

Governments don't think well enough….

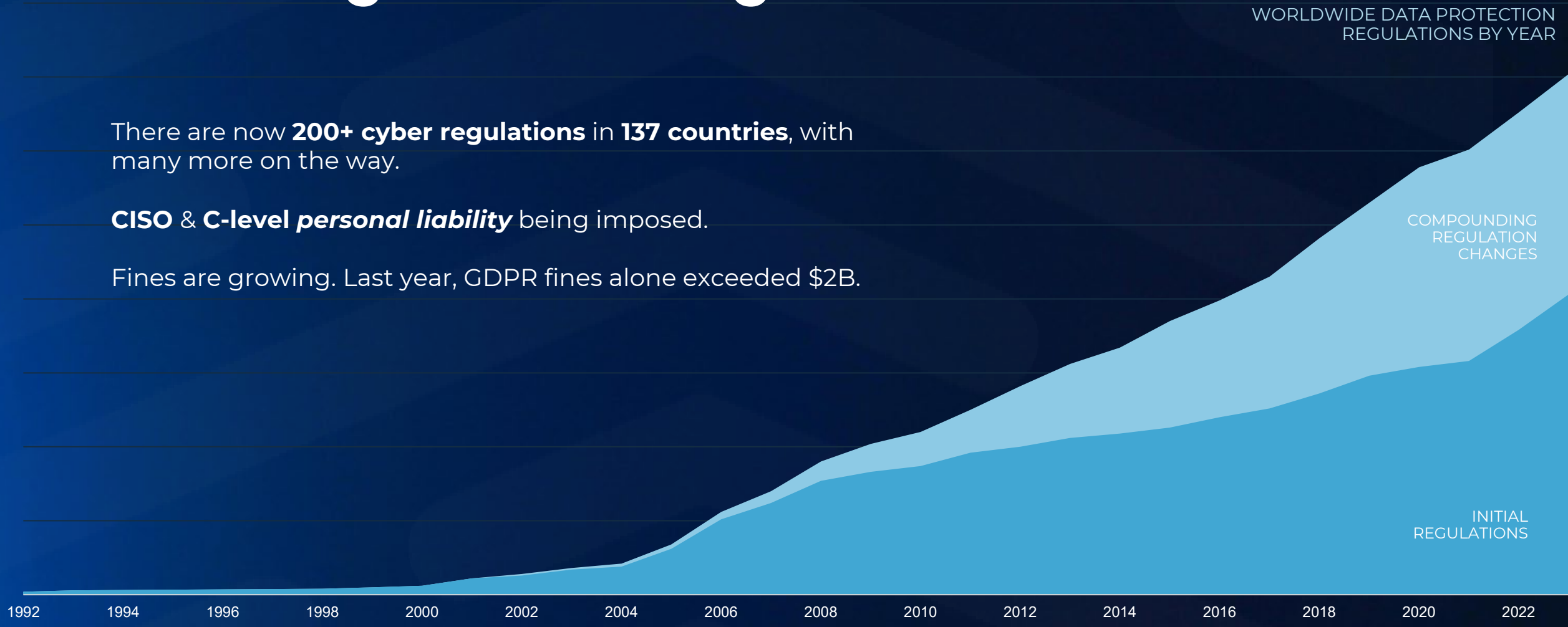
Sources: Momentum Partners, Resilient Cyber, Others, 2022-2024

Governments are imposing a towering wave of regulations

There are now **200+ cyber regulations** in **137 countries**, with many more on the way.

CISO & **C-level *personal liability*** being imposed.

Fines are growing. Last year, GDPR fines alone exceeded $2B.



Source: BreachRx Cyber RegScout™

Are regulations driving change?

DATA

GDPR, 2018

- 2018 EU law that governs how personal data is collected, stored, processed, and shared
- Grants individuals rights over their data, including the right to access, correct, and delete personal information.
- Non-compliance can result in heavy fines, up to 4% of global annual revenue or €20 million, whichever is higher.

This law elevated the importance of data protection and quickly became the de facto standard requiring implementing protection measures, enhance transparency, and prioritize privacy by design to avoid penalties.

Enforcement was initially slow, which took some of the force out of its implementation.

DISCLOSURE

SEC Cybersecurity Rules, 2023

- Publicly-traded companies in the US must now disclose material cybersecurity incidents within four business days.
- Companies must also annually report on their cybersecurity practices.
- The rules apply heightened accountability to executives and their oversight of cybersecurity programs.

These rules have increased the focus on cybersecurity transparency, making it essential for companies to have not only strong protections but also to disclose incidents and their approach to governance.

The requirement for cybersecurity expertise on the Board did not make the final rule, but it has increased executive focus on reporting.

RISK MANAGEMENT

CIRCIA, 2022 & NIS2, 2023

- The laws enforce cybersecurity risk management over critical infrastructure. In the US, that's sixteen industry sectors.
- Both mandate faster incident reporting and continuous reporting requirements.
- Public-private collaboration is emphasized as needed for stronger resilience.

These laws implement more rigorous government oversight over a broad set of the economy, many of which are less technologically-savvy and/or have been slow to invest in cybersecurity measures.

Final rules for implementing CIRCIA are expected in 2025. Resistance to it (plus the election) may impact its final language.

Yes, but...

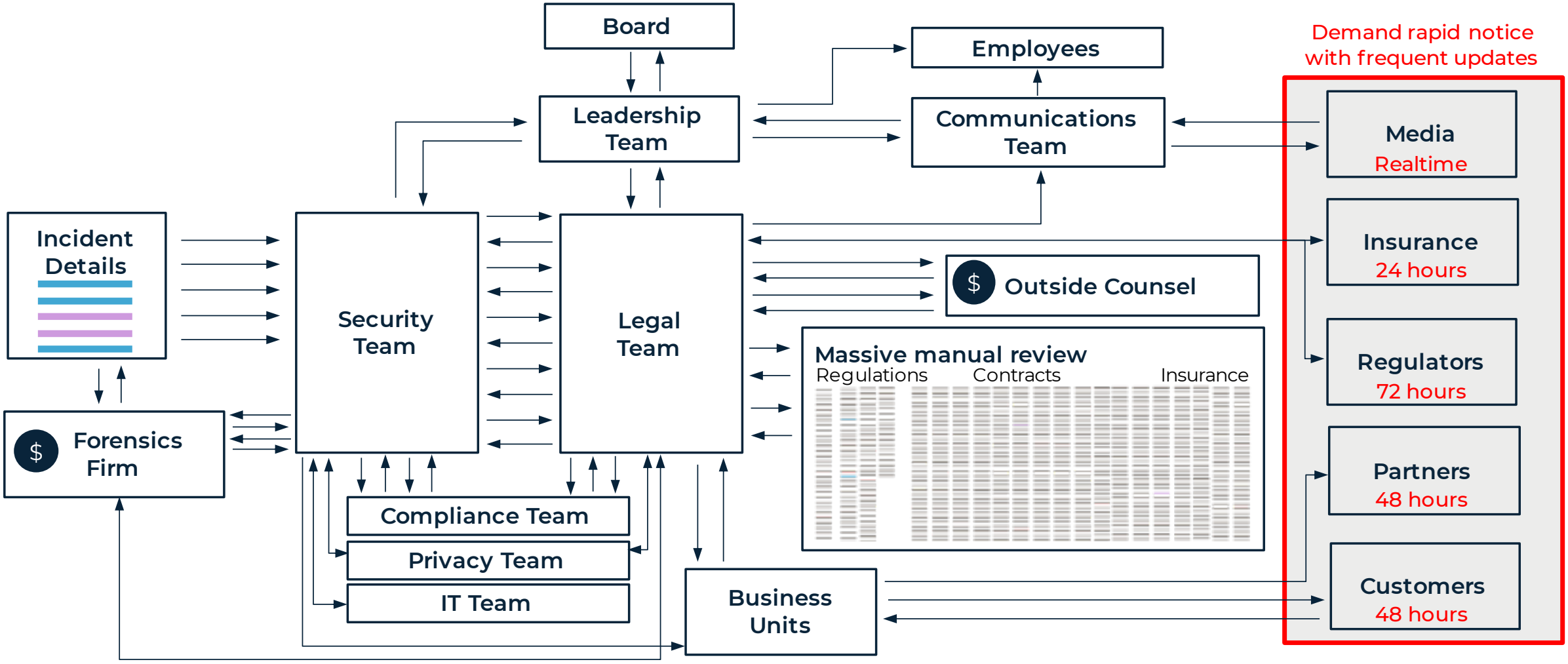
“No company is actually prepared, regardless of their size”

“I’ve never once used a company’s incident response plan”

– Survey of 100+ large law firms

(and their fastest growing practice is … cybersecurity)

Why? The typical response is a chaotic nightmare.



Another view of the legacy “best” practice…

- Business teams think this is technology’s problem to fix, security teams are overwhelmed and rely on heroic talent
- Outdated, uniform, template incident response plan
- Annual tabletop thought exercises with a lot of hand-waving
- Expensive experts on “break-glass” retainers with no context
- Siloed teams with no shared, safe workspace
- Insurers are squeezing down claims

Incident Response is badly broken

This is a business problem.

Yet we still treat it like a technical challenge.
And the cost of a single misstep can be staggering.

~30%

of incident costs are attributable to cybersecurity work

~70%

of incident costs hit the broader business six months to over two years afterward

Source: Cost of a Data Breach Report, 2021-2023

Now: CISOs are held accountable but lose control when a crisis hits.

65%

of board directors believe their organizations are at risk of a material cyberattack in the next 12 months

Businesses expect CISOs to help the business get ready. When a significant event occurs, CISOs in many organizations lose control to legal and business leaders, many who are not properly prepared. Yet CISOs remain accountable and are now facing severe consequences such as felony prosecutions and civil lawsuits.

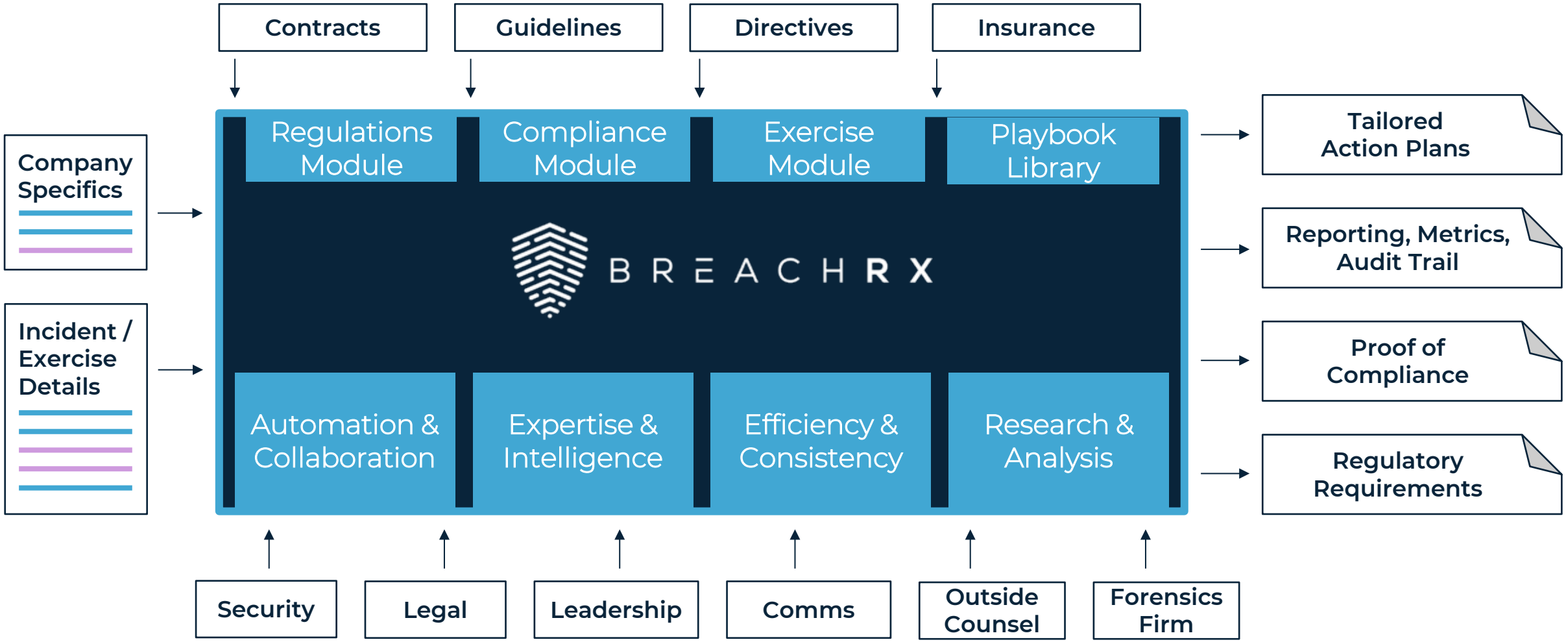
47%

regularly interact with CISOs

Source: HBR/MIT, 2023

THE BREACHRX PLATFORM

Intelligent workflow automation & collaboration for incident response



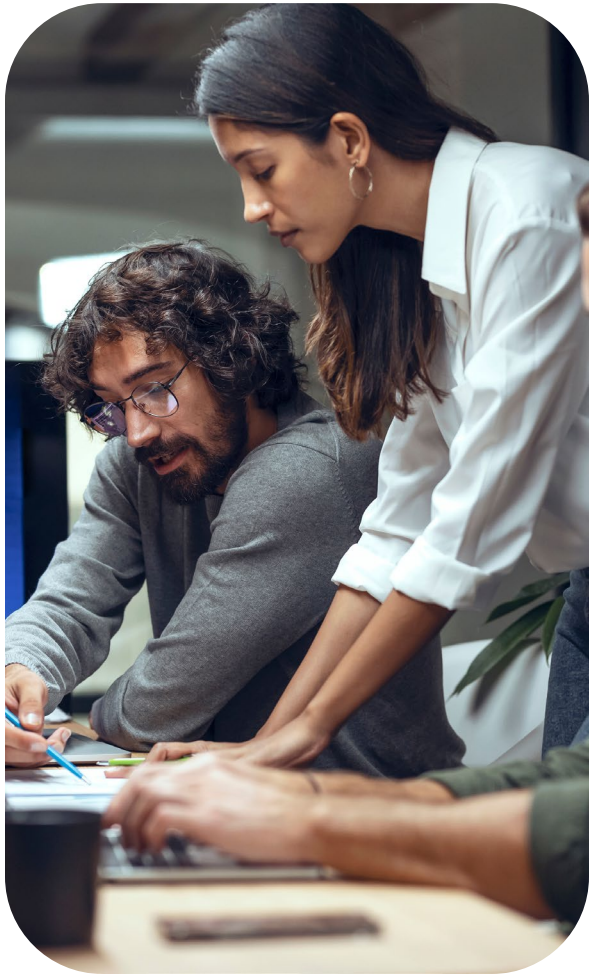
BREACHRX

Companies need to prove they

- ✓ have a sound process
- ✓ consistently follow their process
- ✓ took the right actions at the right time

What you must get right for Modern Incident Response

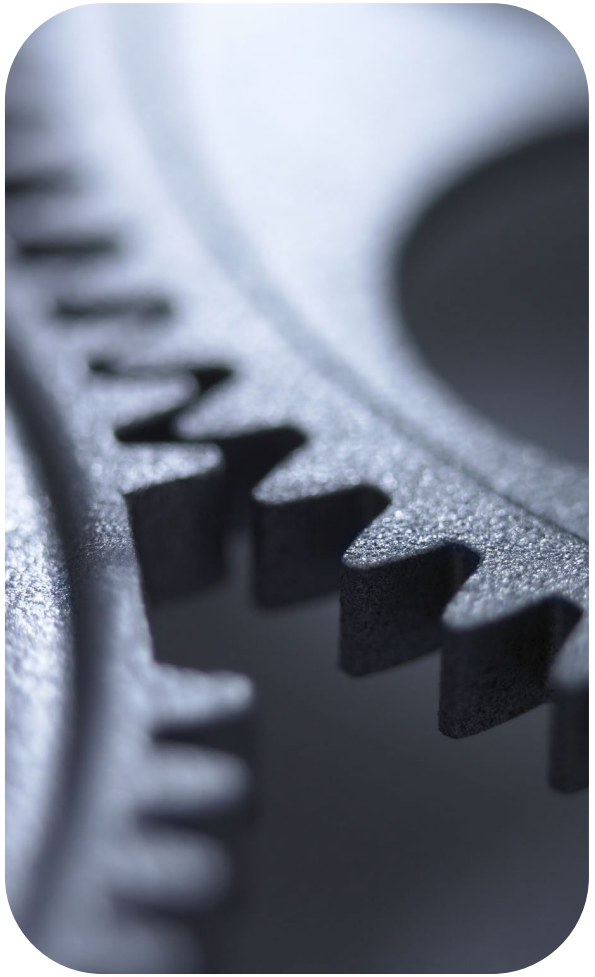
Meaningful Preparation



- **Plans for every type of incident you're likely to face**
- **Proactively prepare for *all* your obligations**
- **Don't just check the box for compliance**
- **Build muscle memory through frequent practice**

Consistency Leads to Efficiency

- **Get teams on the same page—bridge language gaps**
- **Don’t default to what you (and your teams) know**
- **Eliminate single points of failure & tribal knowledge**
- **Centralize decision-making and communications**



Look Beyond Security to Reduce Cost and Risk

- **Protect legal privilege, the right way**
- **Help legal adopt technology**
- **Communications are crucial**
- **Prepare executives for key decisions**

Incident response records are now audited like financial records

CISO, Fortune 500 company

Will you be ready to play back the tape?

Questions?

BREACHRX

Contact Info:
Andy Lunsford
alunsford@breachrx.com