10 Cybersecurity Decisions Every Board Gets Wrong

What 30 years of advising executives taught me about the decisions that actually matter

Chris Thatcher

MARQUE PUBLISHING

Introduction

I've spent thirty years sitting in boardrooms, war rooms, and the occasional conference room with bad coffee, helping executives figure out cybersecurity. Fortune 500 companies, mid-market firms, government agencies — the settings change, but the conversations are surprisingly similar.

Here's what I've learned: most boards aren't failing at cybersecurity because they don't care. They're failing because they're making the same ten decisions wrong — decisions that seem perfectly reasonable in the moment but set their organizations up for trouble down the road. I've watched smart, capable leaders make these mistakes over and over, not because they're careless, but because nobody ever explained the problem in plain terms.

That's what this guide is for. No scare tactics, no vendor pitches, no alphabet soup of acronyms. Just ten decisions I've seen go sideways hundreds of times, and what I'd tell you to do differently if we were sitting across from each other at a coffee shop.

Some of these will seem obvious once you read them. That's the thing about good advice — it usually does. The hard part isn't understanding it. It's acting on it before something forces your hand.

1

Treating Cybersecurity as an IT Problem Instead of a Business Risk

What boards typically do

They assign cybersecurity entirely to the IT department and consider it handled. The board hears about security once a year, maybe twice, sandwiched between budget reviews.

Why it backfires

When a breach happens, it doesn't stay in the server room. It hits revenue, reputation, regulatory standing, and shareholder confidence. If the board hasn't been part of the conversation, they're making critical decisions in a crisis with almost no context.

What to do instead

Put cybersecurity on the board agenda the same way you put financial risk there — regularly, with clear metrics, and with enough context for informed discussion. You don't need to understand packet sniffing. You need to understand what a disruption to your core systems would cost, and whether your current posture matches that risk. That's a business conversation, not a technical one.

2

Measuring Security by How Much You Spend on It

What boards typically do

They equate a bigger security budget with better security. “We spent $12 million last year“ becomes shorthand for “we're protected.“

Why it backfires

Some of the worst breaches I've seen happened at organizations that were spending enormous amounts on security — just spending it on the wrong things. Money spent without strategy is just expensive noise.

What to do instead

Measure outcomes, not inputs. Ask questions like: How quickly can we detect an intrusion? How fast can we recover critical operations? What percentage of our known risks have mitigation plans? A well-run program with a modest budget will outperform a bloated one every time. The question isn't “how much are we spending?“ — it's “what are we getting for it?“

3

Assuming Compliance Equals Security

What boards typically do

They pass their audits, check their regulatory boxes, and sleep soundly. “We're compliant“ becomes the answer to every security question.

Why it backfires

Compliance frameworks are floors, not ceilings. They tell you the minimum you need to do to avoid a fine, not what you need to do to avoid a breach. I've seen plenty of organizations that were fully compliant on paper the day they got compromised.

What to do instead

Treat compliance as a starting point and build your security program around your actual risks, not someone else's checklist. Run tabletop exercises that test real scenarios your organization might face. Ask your security team what keeps them up at night — I promise the answer won't be “whether we'll pass the audit.“

4

Delegating All Cyber Decisions to the CISO Without Understanding Them

What boards typically do

They hire a Chief Information Security Officer and assume the problem is solved. When the CISO presents to the board, heads nod politely and nobody asks hard questions because

they don't want to look uninformed.

Why it backfires

Your CISO can't be effective without board-level support, and the board can't provide meaningful support if they don't understand the basic landscape. When a crisis hits and the CISO needs fast executive decisions — to shut down a system, to notify customers, to engage law enforcement — the board is flying blind.

What to do instead

Invest in basic cyber literacy at the board level. Not certifications, not technical training — just enough understanding to ask informed questions and evaluate trade-offs. A good CISO will welcome this. If your CISO can't explain their strategy in terms a smart non-technical person can follow, that's a different problem worth addressing.

5

Buying the "Best" Tools Instead of Building the Right Program

What boards typically do

They approve purchases for the latest, most highly rated security tools. The logic seems sound: buy the best, get the best protection.

Why it backfires

Tools without processes, trained people, and a coherent strategy are just expensive shelfware. I've walked into organizations running twenty security products where nobody could tell me how they worked together — or if they worked together at all. Meanwhile, the team was drowning in alerts they didn't have time to investigate.

What to do instead

Start with the program, not the product. Define what you're trying to protect, what your biggest risks are, and what capabilities you need. Then find tools that fit. And before you buy anything new, make sure you're getting full value from what you already own. Most organizations are using about 30 percent of the capability they've already paid for.

6

Ignoring Third-Party and Supply Chain Risk

What boards typically do

They focus their security efforts inward — their own networks, their own employees, their own systems — and assume their vendors and partners are handling their own security.

Why it backfires

Your security is only as strong as your weakest connected partner. Some of the most damaging breaches in the last decade came through trusted third parties. If a vendor with access to your systems or data gets compromised, that's your problem, not just theirs.

What to do instead

Build third-party risk management into your security program from the start. Know which vendors have access to your critical systems and sensitive data. Require security standards in your contracts and verify them — not just at onboarding, but on an ongoing basis. You don't need to audit every office supply vendor, but you absolutely need to understand the security posture of anyone with a connection to your crown jewels.

7

Planning for Prevention but Not for Response

What boards typically do

They pour resources into keeping attackers out — firewalls, antivirus, access controls — and spend almost nothing on what happens when someone gets in anyway.

Why it backfires

Prevention is essential, but it's not foolproof. Every security professional will tell you the same thing: it's not a question of *if* you'll have an incident, it's *when*. Organizations without a practiced response plan make bad decisions under pressure — slow to detect, slow to contain, slow to communicate. And those delays are where the real damage accumulates.

What to do instead

Develop an incident response plan and actually rehearse it. Run tabletop exercises at least twice a year with real executives, not just the security team. Make sure everyone knows their role — who makes the call to take systems offline, who talks to the press, who handles legal and regulatory notifications. The time to figure this out is a Tuesday afternoon, not 2 AM during a ransomware attack.

8

Treating Employee Training as a Checkbox

What boards typically do

They mandate annual security awareness training — usually a mind-numbing online module that employees click through as fast as possible — and call it done.

Why it backfires

Phishing and social engineering are still how most breaches start. A once-a-year video isn't going to change anyone's behavior, and deep down, everyone knows it. The training exists to satisfy auditors, not to actually make people more security-aware.

What to do instead

Make security awareness part of the culture, not an annual chore. Short, frequent, relevant training works far better than a yearly marathon. Use real examples from your own industry. Run simulated phishing exercises and treat the results as a learning opportunity, not a gotcha. And most importantly, make it easy for employees to report suspicious activity without fear of looking foolish. The person who says “I think I clicked on something weird“ is saving you millions if you've built a culture where that's encouraged.

9

Making Risk Decisions Without Quantifying the Actual Exposure

What boards typically do

They discuss cyber risk in vague, qualitative terms — “high risk,“ “medium risk,“ color-coded heat maps that look impressive but don't tell you much.

Why it backfires

You can't make good business decisions about risk if you can't put it in business terms. When someone says a risk is “high,“ what does that mean? A $500,000 problem? A $50 million problem? Without quantification, every risk looks roughly the same, and the board has no rational basis for deciding where to invest.

What to do instead

Start quantifying your cyber risks in financial terms, even if the numbers are imperfect. Methods like FAIR (Factor Analysis of Information Risk) can help you estimate probable loss in dollar ranges. When you can tell a board, “This risk has a 15 percent chance of a $20 million impact over the next year,“ they know how to weigh that against other business decisions. Perfect precision isn't the goal — directional accuracy is. Even rough financial estimates are infinitely more useful than a red-yellow-green chart.

10

Waiting for a Breach to Take Cybersecurity Seriously

What boards typically do

They treat cybersecurity as a background concern — important in theory, but never quite urgent enough to demand real attention. Until something happens.

Why it backfires

Post-breach is the most expensive and least effective time to get serious about security. You're making critical decisions under pressure, public scrutiny, and potential regulatory action. The costs — financial, reputational, operational — are orders of magnitude higher than what proactive investment would have been.

What to do instead

Treat cybersecurity with the same urgency you'd give any material business risk. You don't wait for a factory to burn down to buy insurance and install sprinklers. Schedule regular briefings, fund the program appropriately, and make sure the board has enough context to provide real oversight. The organizations that handle cyber incidents best aren't the ones that spent the most — they're the ones that were paying attention before they had to.

If any of these ten decisions sound familiar, you're in good company. I've seen every one of them play out at organizations of all sizes, in every industry. The good news is that none of them are hard to fix once you see them clearly. It's not about spending more money or hiring more people. It's about asking better questions and making more informed choices.

If you want to go deeper — into the frameworks, the conversations, and the practical steps that turn cybersecurity from a source of anxiety into a genuine business advantage — my book *Cyber Risk is Business Risk* lays it all out. You can find it, along with additional resources for boards and executives, at **marquepublishing.com**. Thanks for reading. Now go ask your CISO a hard question.

Continue reading:

Cyber Risk is Business Risk

marquepublishing.com