



MAKING BETTER CYBER RISK DECISIONS

Architecting the Choices



Malcolm Harkins

Chief Security and Trust Officer | Epiphany Systems



“Victory awaits him who has everything in order. Defeat is certain for him who has neglected to take all the necessary precautions in time.”

Roald Amundsen, on the South Pole.

Uncertainty, chaos, and luck – why some thrive despite them all. In the book *Great by Choice*, Jim Collins and Morten Hansen distill a decade’s worth of research into compelling stories and analysis on why some organizations are what they call 10X’rs. They outperform the competition – repeatedly overtime. The best leaders were not more risk taking, more visionary, or more creative, the best leaders practiced Fanatical Discipline, Productive Paranoia, Empirical Creativity, and Limitless Ambition. They made better choices despite being in the same circumstances.

So, how can we organizationally make better cyber risk choices?

In the relentless battle to protect their companies, CISOs must fight on two fronts with two very different adversaries and competing missions - two battlefields in essence. First, there is the external visible battlefield we hear about every day: the threat actors, malware, vulnerabilities, all that type of stuff. The other battlefield is internal and largely invisible: the budgets, bureaucracies, and behaviors within an organization. Navigating this internal battlefield is just as daunting but is more critical to the choices that our organizational leadership must make to manage business risks, specifically, with respect to how we prioritize investments to prevent, detect, and respond to cyber risk.

A story is data with a soul married to both passion and logic. Considering oneself a choice architect – how you architect a choice will determine in many cases the outcome of the idea presented. Maybe a better business friendly way is to say “I am an options architect – how I architect the business options for the way security choices are made will determine the likelihood of a successful outcome for my stakeholders”. Therefore, the soul of the CISO must be both a choice and options architect to manage any battlefield, using passion and logic equally to arrive at outcomes.

The reality is that only some decisions are the CISOs to make. More often other managers make the key business decisions, and CISOs must work to influence those decisions - sometimes in a different direction. And the measure of success is often a question of how well you tell the story, how you evoke an emotional response, and how you portray the risks and rewards in the right context. Examples can include the risk to the business, the risk to the brand, the risk to the privacy of your customer’s data. It may even be on a larger scale like policy decisions regarding societal risks to privacy and security rights. Because they’re all different risks and potential cost portraits, how you tell that story will evoke a different response and directly influence different outcomes. Your approach will frame not just the immediate decision made, but the impactful subsequent decisions people will make.

We want to marry the business problem as well as the solution choices as the soul of the story.

Choice architecture describes the way in which decisions may be influenced by the different communication techniques (passion and logic) at our disposal as to how the choices are presented, and is a term used by Cass Sunstein and economist Richard Thaler in the 2008 book Nudge. Sunstein and Thaler state that a choice architect has the responsibility for organizing the context in which people make decisions and that there is no such thing as a “neutral” design. Small, and in some cases apparently insignificant, details can have a major impact on people’s behavior and thus the choices they make. As with other studies on choices and decisions, Sunstein and Thaler share that it is “reasonable to assume people make good choices in contexts in which they have experience, good information, and prompt feedback. They do less well in contexts in which they are inexperienced and poorly informed, and in which feedback is slow or infrequent.”

Let’s continue the journey and look at “why”. Just like Simon Sinek’s famously titled book, “Start with Why” he states, “if we’re starting with the wrong questions, if we don’t understand the cause, then even the right answers will always steer us wrong.” So, we must “start with why”. We want to marry the business problem as well as the solution choices as the soul of the story. Why does the organization we support exist? Why does the security team exist? While these may appear to be simple questions, it has been found in some cases that “the why” the security team exists, that the definition of our mission is not well aligned with the business. If we are not aligned, we won’t be architecting choices well and therefore, our decision path and the decisions the business makes will be wrong – adding more risk and generating more churn on the aforementioned internal battlefield of budgets, bureaucracy, and behaviors.

Over 20 years ago, having the role of choice architect as CISO where the IT security and business continuity information security mission statement was along the lines of **“Safeguard information assets ...”** that was difficult to remember then, never mind today.. No one else remembered it either – especially across the lines of business within the company. Therefore, information security was a cost, it got in the way, it was a necessary evil and an afterthought for everyone. However, 911 changed the world – it became relevant to mitigating material cyber risk to the business. One would say this mission was a **1st generation approach to information security**. By late 2003, it became apparent that the soul of the story was starting to get stuck in this role as a choice architect- unable to push ahead on the internal battlefield despite the premonition of a “Perfect Storm” of Information Risk that was on the horizon in which the company had been warned about since mid-2002. In preparation for the first board discussion on information risk and security, a choice was made to be rather pithy in the review – having only 30 minutes to explain everything.

A BIT OF THE PAST, THE PRESENT, AND OF COURSE THE FUTURE

The weeks of preparation leading up to the board meeting was a struggle. We had made good choices and decisions the prior couple years, but we were on the verge of making some very poor decisions – both for the business and on cyber risk. We had respectively lined up with perspectives that had win-lose not win-win outcomes. The question was what to do about keeping the soul but changing the outcome narrative (passion and logic) in this story. We needed to really think about WHY the information risk and security team existed. We were not ready to have the conversation. After a lot of thought and discussion with mentors, the management, and the team, we realized why. What should have been obvious years earlier but wasn't – our mission – our WHY was to **Protect to EnableSM**. It became so clear and we transformed. We then started to architect a better story. We entered **the 2nd generation of information security**. We made better choices. We made better decisions.

The core of business-driven security and the mission of the information risk and security team is “Protect to EnableSM.” When you are protecting to enable people, data, and the business, you are proactively engaged upfront and aligned with the business on the evaluation of how to achieve the business objective, while best optimizing your costs and controls.

Below, as shown in Figure 1, is the “9 Box of Controls” approach to understanding how risk and cost drive controls, which was published in September of 2016 in the second edition of my book – “Managing Risk and Information Security: Protect to Enable”. The 9 Box of Controls includes some actionable perspectives to align on outcomes with the business. Conversations with peers at other companies over the years have validated this view. Many of them are now using the 9 Box to drive both tactical and strategic choice architect discussions in their organizations on where they are spending their resources today, and where they should be headed long term.

Risk increases as we move from prevention, to detection, to response. Cost increases as we move from automated to semi-automated to manual controls. (See Figure 1 below)

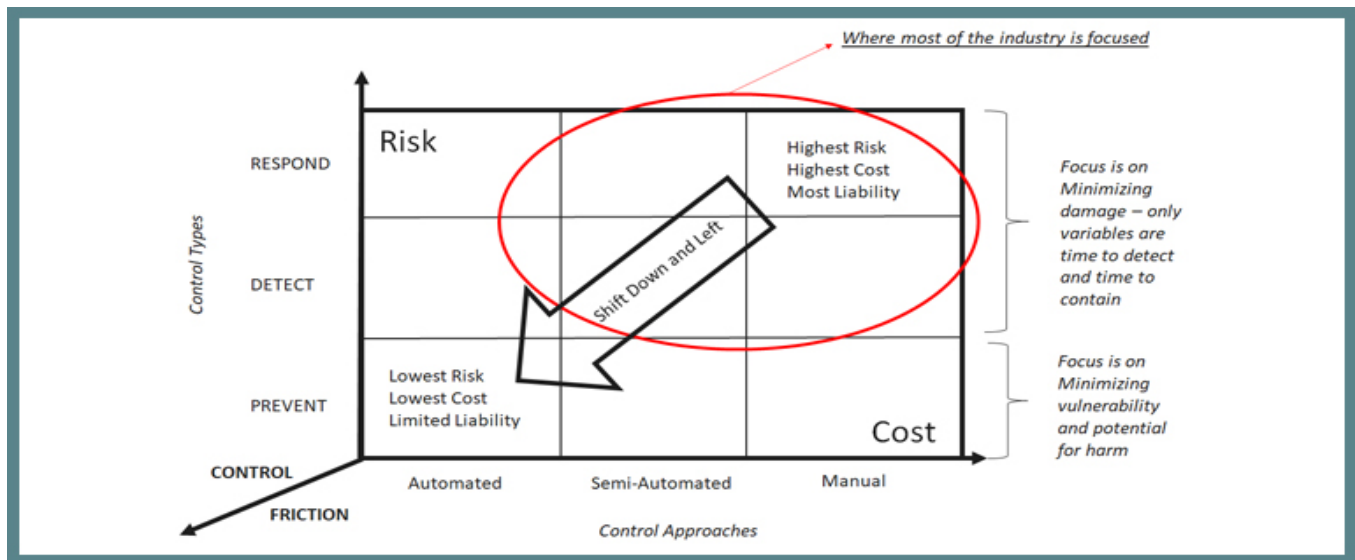


Figure 1: 9 Box of Controls

A NOTE ON CONTROL FRICTION – PERHAPS THE CORNERSTONE OF BUSINESS ALIGNMENT

There is a third dimension to the 9 Box: control friction. Friction is defined as the force that causes a moving object to slow down when it comes into contact with another object. Similarly, controls can impose friction or “drag” on business velocity—they can slow the user or a business process. However, friction is not a fundamental, immutable force like gravity. Instead, we can determine exactly how much control friction we apply. Apply too much and business users may choose to circumvent security controls; adding cost, but also risk; because the security team lacks visibility into the technology being created or used. So, not only can we not prevent vulnerabilities or compromises, but detection becomes difficult due to lack of visibility, and in many cases, response after the fact becomes the only option.

If a business adheres to high-friction controls, the long-term effect is consistent generation of systemic business risk. High-friction controls generally hinder business velocity; the organization can lose time to market and the ability to innovate, and over the long term it may lead to the loss of market leadership.

Put yourself in the role as the choice architect and go to your management with an investment request for information security where you commit and demonstrate how you plan to lower risk, lower total cost of controls, and improve business velocity. The business outcome will be a better set of choices and collectively we would make better decisions.

Unfortunately, we cannot simply stop there. We collectively need to transform perspectives. We need our executive leaders to embrace and embed in the fabric of our organizational culture what the author calls, **“Secure to Succeed – the 3rd generation of information security”**. When the organization adopts a Secure to Succeed approach, we will have arrived at a level of maturity where the business intrinsically understands what is at stake, is

committed to managing the cyber risk exposure and accepts both the social responsibility in addition to a fiduciary one. Stepping well past the basic compliance requirements is done, not because they need to, but because they know it is the right decision to go on this journey.

So what, now what? How do we do this? How do we get to the next level of better choices and better decisions? First, we keep in mind what has been mentioned above from Sunstein and Thaler. It is “reasonable to assume people make good choices in contexts in which they have experience, good information, and prompt feedback. They do less well in contexts in which they are inexperienced and poorly informed, and in which feedback is slow or infrequent.” We need to improve our data, analysis, and provide more accurate and timelier context that the business can understand. Second, remember a story is data with a soul married to passion and logic. We must tell the right story to motivate others to action.

Accurate and timelier context for choices is all about the three P’s.

1. **Predictive:** so we can be proactive ahead of the risk curve(s) coming.
2. **Preventive:** so we bias ourselves towards a true reduction in the risk of a material exposure.
3. **Prescriptive:** so we can simplify the actions that can be chosen to mitigate the risks.

Storytelling is all about the three F’s.

1. **Framing:** so we can reduce the complexity and improve the understanding of our risks.
2. **Focus:** so we can pinpoint with precision the options we have to mitigate material exposure.
3. **Facilitation:** so we can actively guide decision makers connecting the dots across the enterprise.

One final note that is often misunderstood when making a risk decision/choice: **accepting risk is a business process, it is not a control.** When you accept a risk, you are making an explicit decision, often using an implicit form of consent that results in no formal assignment to the risk owner to be prepared should the risk manifest. Many risk decision makers DO NOT realize this to be the case, thus the organization is not properly prepared to respond – leaving the gates wide open to material impact and exposure – not only to the organization but in some cases to society.

If you don’t make a choice ...the choice will always make you. In security, there is a corollary to this. No decision is a decision and the CISO is generally the fall guy. 🗑️

ABOUT THE AUTHOR



Malcolm Harkins is Chief Security and Trust Officer at Epiphany Systems. He is responsible for information risk and security including security and privacy policies, peer-outreach activities to build understanding of cyber risks, and best practices to manage and mitigate those risks. Focus areas include the ethics of technology risk, social responsibility, total cost of controls, and industry accountability. Malcolm is an independent board member and advisor to many organizations. Malcolm served as Chief Security and Trust Officer at Cylance and was Chief Security and Privacy Officer at Intel. He is the author of Managing

Risk and Information Security: Protect to Enable, now in its second edition.

