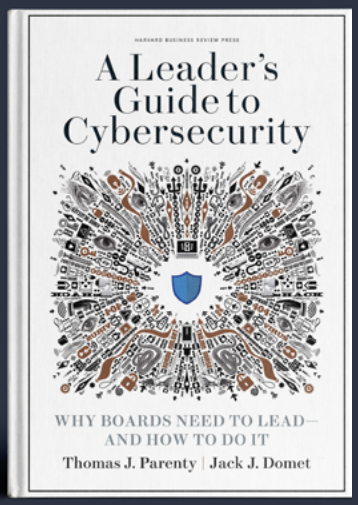
Praxonomy

BOOK REVIEW



A Leader's Guide To Cybersecurity

★★★★★

"It's a good book, a very good book in fact. Parenty and Domet know what they're talking about and have strong views on how any board member can step up and do the right thing. This book is well worth the read, whether you're a board member or not."

- Jay Shaw

A Leader's Guide To Cybersecurity: Why Boards Need To Lead — And How To Do It
by Thomas J. Parenty and Jack J. Domet
Harvard Business Review Press ISBN: 9781633697997

DUTY OF CARE

Though they make the point in diplomatic language, the authors assert, up front and unequivocally, that company directors are responsible for cybersecurity; the logic being that boards are responsible for their organizations' overall approach to risk and that technology vulnerabilities comprise a big and growing part of corporate risk.

Thus, your responsibilities as a director cannot be ignored, deferred or delegated. It's on you, now and in the future.

If you tell yourself that you can rely on the good work and recommendations of your IT staff and call it job done, then you are derelict in your duty as a director. If you decide to rely only or mostly on third-party tests, audits and certifications, then you are derelict. If you think that you can buy security by outsourcing key decisions to consultants or suppliers, then you are derelict. In short, if you think that you, as a board member, do not carry key, personal and ongoing responsibility for leadership in the cybersecurity of your company, then you need to think again.

IT'S ABOUT THE FRAMING

Some directors believe that cybersecurity is an information technology issue best left to experts. This is not surprising given that most board members are not IT security practitioners, computer system administrators or the like. They don't speak the language. They are not necessarily up to date on technical standards, hardware and software options, the latest news or industry best practices. Feeling out of their depth, some directors decide to leave it to the executive team or other board members to deal with company IT security policies and procedures.
This, the book says, is a mistake. Cybersecurity is not about IT issues per se. It's about risk, specifically the risk of interruptions to and failures of critical business functions. For example, Company X may have thorough and well documented back-up procedures but unless those procedures are regularly tried and tested, nobody knows how well they will stand up in an emergency. It's the board's job to ask, to see that meaningful tests are carried out and to make sure that lessons learned are incorporated into company operations.

This kind of oversight brings immediate and powerful benefits. Companies whose back-up systems work well cannot be so easily brought to their knees by ransomware or related attacks, not to mention by the inevitable employee mistakes and equipment failures that all companies suffer at one time or another.

TELL ME A STORY

Useful framing for board-level oversight often takes the form of narrative. The first step is to list the company's critical business functions. Then the board needs to start thinking about what might go wrong and who or what might be in position to make those things go wrong.

These steps are followed by thinking through "What if?" and "What next?" scenarios. If a critical business function goes down, what are the consequences? the company's responses? the possible costs? the timelines? the worst case? the communications process? — and more.

In the end, the board should be building collections of cybersecurity stories — each a fully developed narrative with a beginning, middle and end, a list of characters, their profiles and motives, plot and context, along with discussions and plans for corrective and preventive actions and policies.

The process is not unlike what happens when a team of writers sits down together to create scripts for a television series; they conceptualize the set-up and start writing episodes.

Not every story has to be written at once. Neither do the board's first attempts have to capture every possible consequence of a mishap to a critical business function. The point is to get started.

AIDES-MÉMOIRE

The book, which shines when it comes to practical advice, includes tables, guides and plenty of war stories to focus the mind and point the way. It is clear that the authors' simple, practical advice is born of decades of work in the field. The result is an extended how-to, a handbook that manages to be both readable and easy to put to immediate use.

This is not a small accomplishment. 30 years ago IBM adopted a process called Component Failure Impact Analysis (CFIA), a framework that takes a hard look at the various parts of IT systems in which a single component failure might disrupt or destroy, well, everything.

IT project leaders still use CFIA methodology to assess the consequences of component failures and devise possible mitigations. But CFIA is not for everybody. It's hard technical work.

CFIA provides tools for engineers to analyse IT systems while the book helps boards look at key and core business functions. Both methodologies look to assess the potential impact if and when an underlying process is disrupted, by a cyber-attack for example, and then think through what could be done to prevent or recover from the damage.

In short, the book achieves its aims by explaining, in simple, non-technical terms, how boards can go about assessing their own critical business function vulnerabilities and then build plans to protect those functions from failure and attack while creating a resilient, forward-looking corporate culture.

It's not that the authors have invented something entirely new but rather that they have distilled industry best practices and the lessons from their own hard-won experience into a useful primer for the non-technical board member. It's impressive work.

BEYOND THE BOOK

Board members have cybersecurity responsibilities that go beyond the core business functions of the company.

In many cases boards themselves needs better IT support. In fact, there is an argument for putting board work and communications on entirely separate, high-security systems. This would help shield the board from the risk of both external and internal breaches and allow the board to keep working even when the company's own systems have been compromised.

A board member's personal digital hygiene can usually benefit from an upgrade or two (or three). It is not difficult to start taking basic precautions. Every board member should do so.

There is also a case for top-level leadership in regard to increasing stakeholder data protection in the company itself along with an opportunity for public advocacy of better data protection rights in the broader community, both on a personal and full-board basis.

The list goes on but core company cybersecurity is a great place to start, arguably the best place to start, and this book is a great first step on the journey.

About the Reviewer
Jay Shaw is the Founder and Chairman of Praxonomy. Jay is a serial entrepreneur with over 20 years experience in the IT industry. Prior to founding Praxonomy, he was the Co-founder and CEO of NetDimensions, a London Stock Exchange AIM listed enterprise software company. Jay also serves as the Non-executive Chairman of SandSIV Group, a software and services company based in Zurich, Switzerland.