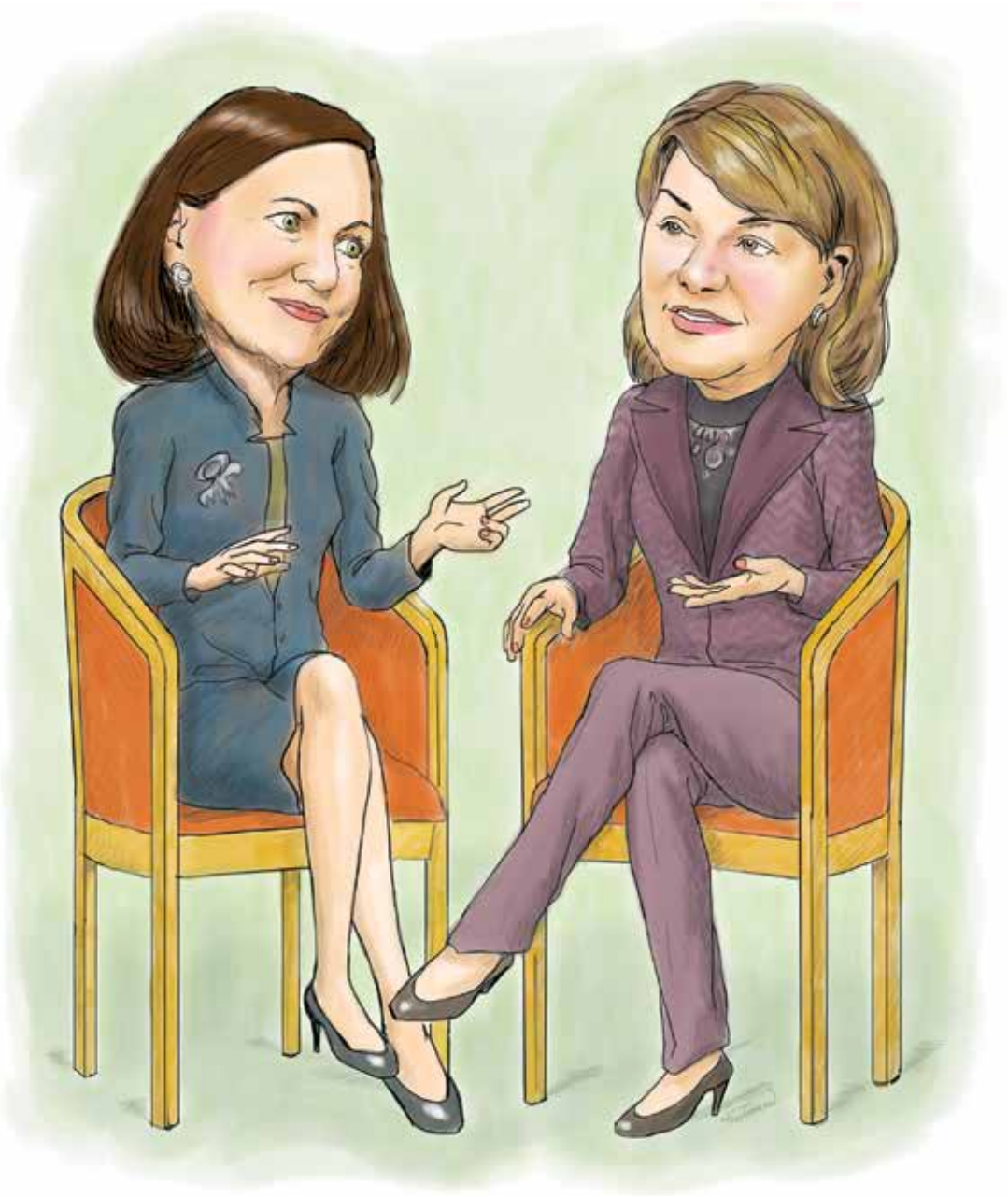

Talking About Cybersecurity Execution

A board advisor and a former military commander demystify cyber risk.

Edited by Judy Warner

Suzanne M. Vautrinot was talking about cybersecurity long before many of us had heard the word, much less understood the growing vulnerabilities of our networked computer systems and devices. Now a director for three very different companies, the retired U.S. Air Force major general was commander of the 24th Air Force, Air Forces Cyber, and Air Force Network Operations. Upon leaving the military, she was invited to join the boards of the public companies Symantec and Ecolab, and the private engineering, construction, and services company Parsons Corp.

Mary Ann Cloyd is the leader of PwC's Center for Board Governance, which advises boards and audit committees on emerging issues and best practices. Before accepting her current position in 2012, Cloyd held various client service and operational roles over the course of three decades at the Big Four audit and accounting firm. She has also served on both PwC's global and U.S. boards of partners and principals. *NACD Directorship* brought these two dynamic and informed executives together to talk about issues related to cybersecurity.

ILLUSTRATION BY JT MORROW

Mary Ann Cloyd: In the context of the boardroom, I think you must look at cybersecurity differently based on your military and varied board experiences. Let's start there.

Suzanne M. Vautrinot: The dialogue on cyber has undergone a fundamental change. In the early days, there was a trust factor with the World Wide Web. Unfortunately, there are always those who take advantage of our trust, and the age of web-enabled criminals, or hackers, was born. We had to think differently about technology, design, and application. Not because the capabilities weren't still extraordinary, but there was an added factor, a recognition that there's risk as well as opportunity. Therefore, let's implement technology security solutions in a way that makes that risk manageable and helps protect that which is of the greatest concern to our business.

Cloyd: So, have the bad guys gotten way out in front of business? Because it does seem like this whole dialogue has changed and that cybersecurity is much more front and center even in the last 12 or 18 months. Is that true?

Vautrinot: It's absolutely true that it has become a key area of discussion, and I believe that's a good thing. What we discuss and understand leads to appropriate action. For example, we can break down cyber-risk elements into three categories: human error, system vulnerabilities, and direct attacks. The first two represent the greatest percentage of what the military would call an "attack vector." They apply to all businesses and can be addressed with policy changes as well as technology. The third is "targeted"—a bad actor is specifically after your business or sector. Based on your business, geography, etc., you're going to look at these threats differently. How dependent is your business on network and automated systems, and in what parts of your business? An R&D organization, a manufacturer, a retail company, a financial institution, and a critical utility would likely have different considerations regarding cyber risk. Certainly, some of the solutions and security technology can be the same, but it's not a cookie-cutter approach. An informed risk assessment and management strategy must be part of the dialogue.

Cloyd: This is one step toward demystifying cybersecurity. I really want to hear your perspectives on what management and the board need to be doing to effectively address cyber risk.

Vautrinot: Most simply, getting comfortable in a cyber-risk dialogue with management as well as experts or partners. I am on three very, very different boards. What's common to each are the similar interests and conversations with the C-suite regarding appropriate organizational structure, security of systems, financial controls, employee/vendor interface considerations, security of intellectual property, and resilience of corporate data and processes. And perhaps during a potential acquisition or restructuring, there's also discussion on information security and protecting confidentiality. There are, and should be, unique discussions in every company. For example, you'd expect the largest cybersecurity company in the world to have conversations on growing technical capability and a deeper understanding of the behaviors and constantly changing methods used by bad actors, with an imperative to improve security and confidence for its customers. And they'd consider reputational risk, because even if you provide the best technology, if your customer isn't using the most recent version or isn't using it in the way that it was intended, then there is a reputational risk back to your company when trouble occurs.

In a corporation that builds critical infrastructure, the cybersecurity dialogue extends to design considerations for industrial control systems for bridges, airports, dams, etc., and even led to the acquisition of companies with special skills to apply to these uniquely physical issues. In a company with extensive R&D capability and intellectual property, you'd expect the protection of critical information to have special consideration.

Cloyd: This is very different than the way business has operated in the past. The competitive advantage gives way to mitigating a risk that is anathema to all.

Vautrinot: Exactly. You'll find that the chief security officer or chief information officer—whatever organizational structure is being used—these folks talk to each other informally and formally. And because it started to be a government concern in national security long before businesses, they talk to their government equivalents. It is a continuum of the same conversation that is anathema to us all: shared interest and shared solutions.

Cloyd: You can be of great help to the director community at large because not every board has a Suzanne Vautrinot. There aren't enough of you in the world.

Vautrinot: When we as board members are dealing with something that requires true core competency expertise—whether it's mergers and acquisitions or banking and investments or cybersecurity—there are advisors and experts to turn to because it is *their* core competency. They can facilitate the discussion and provide background information, and enable the board to have a very robust, fulsome conversation about risks and actions.

Cloyd: So outside advisors and consultants can help facilitate the discussion between the board and management, as well as provide background information so the board can have that robust and fulsome dialogue?

Vautrinot: All of the above. The board needs to be comfortable having the conversation with management and the internal experts. They need to understand how cybersecurity risk affects business decisions and strategy. The board can then have a conversation

Mary Ann Cloyd

Cybersecurity "is like other business risks that you're assessing, evaluating, and dealing with. It's another part of the risk appetite discussion."

with management saying, "OK, given this kind of risk, what are we willing to accept or do to try to mitigate it? Let's have a conversation about how we do this currently in our corporation and why."

Cloyd: What you just described doesn't sound unique to cybersecurity. It's like other business risks that you're assessing, evaluating, and dealing with. It's another part of the risk appetite discussion.

Vautrinot: Correct. The only thing that's different is the expertise you bring in, and the conversation you have may involve slightly different technology.

It's also important to understand that the discussion is about a technology that is probably pervasive in your business and was built before the technologists were asked to consider cybersecurity as part of the risk. They were asked to provide a system that enabled communication or marketing or expanded business functionality, probably at the cheapest cost possible. Now, we have a different set of concerns: can we adapt what we have to achieve cybersecurity where we want to, or do we need to do something completely different?

Cloyd: Cybersecurity is like other risks, so don't be intimidated by it. Just put on your director hat and oversee this as you do other major risks.

Vautrinot: And demand that the answers be provided in a way that you understand. Continue to ask questions until you understand, because sometimes the words or the jargon get in the way.

Cloyd: We have seen in our annual corporate director survey that more boards are bringing in outside expertise to help, as you said, facilitate the conversation. The dynamics and technology are changing so quickly. And it doesn't mean that you don't trust what management is telling you. Another point worth discussing is the tension between managing current profits and investing in infrastructure or operations. What are your thoughts on that and the board's role in the discussion?

Vautrinot: I agree that it isn't a lack of trust in management. Rather, it's a changing environment that requires a change in focus. First, let's talk about money, because we had to do this in the Air Force. There's a big difference between ongoing operating money and a big capital expenditure. This is particularly problematic when an activity isn't "core" to the mission. For the military, it's not a ship, it's not a tank, and it's not an aircraft, yet it's foundational to whether those systems can operate. Just like the military, cybersecurity is not the primary business of most corporations. You know that for Symantec, this is their core business, but for Ecolab or Parsons, it's not. And yet cybersecurity is integral to their operations and ultimately to their success, so it may require enterprise adjustments. This is a prioritization dilemma, and a potential source of tension.

But it's not just about money. It's also about policy changes and authorities and what employees are allowed and enabled to do. You start to talk about things like BYOD [bring your own device] and mobile systems, and emailing from home into the corporate account or emailing from the corporate account so that you're able to work at home, and that raises new levels of concern.

Cloyd: So, among the first questions you as a board member have to be asking are, does the company have the right organizational structure, and what systems are connected to the network?

Vautrinot: Right. The red flags are different. The systems engineers and technologists need to be watching for aberrant or hacking behavior, or when software operations are not consistent with what the software code was designed to be doing. Those are things you have to go looking for actively. You can find it if you're looking for it, but you need the right expertise and you need the right kinds of software and security systems. When you do see anomalies, you need the right kinds of forensic systems to look into the past at the logs both inside and outside your networks. But it is achievable.

Cloyd: Said differently, if you're an engineering company that has to deal with safety issues, you pay for the training and you pay for the supervisory systems and you pay for the monitoring systems or the cameras with the external security. But it's also changing the mind-set and maybe even the corporate structure. The board can't make this happen. This is a management duty. The board's job is, again, to ask those questions.

Vautrinot: Yes, it's a different way of thinking about the problem, and there's potentially an expenditure of resources, a change in corporate policies,

specialized training, and then considerations in how you measure or observe that there has been a change in behavior.

Cloyd: That is such an insightful comment: it's not just what is spent on the technology that needs to be determined, but also what to invest to change the culture and mind-set of the company.

Vautrinot: Culture and behavior are tough to change. The next consideration is core competency. Assuming you require new expertise or capability, do you want to have it internal to your company—which is difficult to get and keep current—or are you going to leverage a third party because that is their core competency, as a partner, by subscription, or through purchases? That decision about internal versus external is tough for some companies, because you know who's on the inside and whom you'll trust, but it may be advisable to trust someone else.

Cloyd: What are your views on where cyber risk needs to be overseen? Is it a committee duty—and if so, which committee—a full board responsibility, or some combination?

Vautrinot: When you want to make a major cultural shift, which this is, you need to bring it to the top level to demonstrate resolve and also to facilitate more rapid adoption. This isn't a passing fad. Safety, when it was first instituted as a corporate focus and regulated imperative, is a good analogy. After establishing and nurturing the new focus, it can then be devolved back into the more standard structure and become an execution responsibility at all levels. It's also important to understand that the technology might be disruptive. The first time that you say, "I'm sorry, but we're not going to allow normal email traffic from home to work," or, "We're going to check the quality of the carrier on your home computer as you make the connection, and if it doesn't have certain levels of security, or if there's an indication of malicious software on your home computer, the corporate system won't allow you to connect." When you start to implement those kinds of policies, you have to make sure everyone's on board, and that means from the C-suite on down.

Cloyd: Cybersecurity is a business issue, it's not just a technology issue. These policy, technology, and expenditure pieces are all part of the solution. You may need slightly different advisors depending on the conversation, and then you may have to decide, do I want this to be part of the internal expertise I have in my company, or are we going to leverage someone else's expertise? Any other advice you have for directors that we haven't covered?

Vautrinot: I'd reiterate that the corporate culture piece is important because, in general, people don't like to be restricted. Employees in many organizations, government and corporate, don't feel personally responsible for cybersecurity. They think it's the CIO's or IT's job. I had lots of young airmen and women working for me and, even though we issued all sorts of policies and told folks you can't use the USB port, people said, "Well, that's not a problem. If I'm not allowed to use this thumb drive, I'm just going to take this computer and plug it into this other port right here, and that will be OK."

Cloyd: So they just turned their computer into a thumb drive?

Vautrinot: Exactly. I like to say, "You can't regulate stupid." That's the other part of this. You have to strictly enforce the behavior, and sometimes it's best to accomplish this with automation. When we created the network for the Air Force, we actually had visibility on how we were using the network. If someone added a device to a USB port, the system would issue an automatic alert or any unauthorized device that went into the USB port shut down the interface.

Cloyd: You need policy, training, and enforcement—in that order. And cybersecurity also is a cultural issue. What else can corporate America learn from military management?

Vautrinot: First, have management facilitate an investigation. Not pejoratively, but to gain information on what's happening on the behavioral network. Give the folks who manage the network the tools to see that behavior and articulate it. This gives them situational awareness and an ability to see what's happening. Then management can have a conversation with network managers about what behaviors are acceptable and what are not. Network managers should have the authority to drive policy and see if that policy is being accepted. A couple of "examples" can go a long way to adjusting behaviors.

Suzanne M. Vautrinot

"Assuming you require new expertise or capability, do you want to have it internal to your company—which is difficult to get and keep current—or are you going to leverage a third party because that is their core competency?"