RANE and Nasdaq Virtual Summit: Rebooting Your Board's Cyber Survival Skills

A Recap of the Event Held on December 8, 2021

February 2022

RANE
Risk Assistance Network + Exchange

Nasdaq

RANE and Nasdaq Virtual Summit: Rebooting Your Board's Cyber Survival Skills

A Recap of the Event Held on December 8, 2021

February 2021

Opening Keynote Interview: Cybersecurity and Board Responsibility — A Conversation With Jay Clayton

Recently the head of the NSA predicted that the U.S. will face ransomware threats every day for the next several years, a reminder that companies face increasingly sophisticated cyber threats from both nation-state actors and cyber criminals.

As the range of cyberattacks become more common, everyone is looking to improve their cybersecurity knowledge, not only for improving their defenses and protecting their businesses but also for enhancing their ESG scores, improving their credit ratings, and increasing their overall resiliency.

In December 2021, RANE and Nasdaq held a virtual summit entitled Rebooting Your Board's Cyber Survival Skills. The highlights and key takeaways from each session are summarized below.

Byron Loflin, Global Head of Board Engagement at Nasdaq, introduces **David Lawrence,** RANE Founder and Chief Collaborative Officer, who interviews **Jay Clayton**, Sr Policy Advisor & Of Counsel at Sullivan & Cromwell and Former Chairman of the U.S. Securities and Exchange Commission, in this opening keynote: Cybersecurity and Board Responsibility.

Byron Loflin began the summit by stating some key facts: "roughly 50% of companies in 2021 have experienced some ransomware or hack threat" and "at least 86% of us have clicked by accident or from temptation on some phishing scheme." He further explained how RANE offers services to board members for corporate oversight and cybersecurity risk assessment.

David Lawrence then introduced **Jay Clayton** and asked him to discuss main themes in cybersecurity and key points conveyed to boards of directors.

- **Clayton** considers cyber risk part of national security and the "general consumer welfare operations" of the economy; issues which can be dealt with through cooperation between the public and private sector. These sectors generally are approaching risk differently; "oftentimes the regulators and government officials you're dealing with on the macro issues are different from the regulators you're dealing with on those micro enforcement type issues." By increasing communication and recognizing systemic issues, organizations can gain consistency and cooperation.

The time to prepare for cyber incidents is not in the moment, therefore preparation for such events is crucial. **Lawrence** noted "the importance of a degree of collaboration, cooperation with government authorities, which also suggests that it is helpful and uncommon for board members to understand."

- **Clayton** said the table top exercises are invaluable to preparing an organization.
- When cyber events happen, organizations will be focused on stopping damage and identifying the source, but there are additional aspects companies have to focus on. Such as employees, customers, inventors and regulators, where corporations come to play to ensure resiliency.
- **Clayton** observed this in boardrooms and the SEC. By preparing scenarios, organizations will have a better understanding on how to

get in touch with the right resources for each type of incident.

Public companies are prepared due to regulatory expectations, and **Lawrence** noted there is "a clear message that's gone out to public companies, but also privately held companies that, at least for the time being, this is the threat environment and we expect you to be prepared."

- **Clayton** went on to comment that "we would expect a board of directors to be overseeing, not managing, but overseeing preparedness. And sometimes we mix that up, that the role of the board of directors is not to be cyber experts and be able to respond to every type of cyber event, but rather to ensure that management is putting in place the tools that they need and preparing and updating and assessing from time to time whether they are ready, whether they know how to deal with it, practicing and the like. I think too many times we mix up the role of boards and management, it would be very difficult for a board of directors that meets six, eight, 10, 12 times a year to be ready to be the cyber triage team, but it's not difficult for the board of directors to be asking those questions and ensuring that management is giving good answers."

Cyber attacks will continue to be a part of the threat environment because they are low risk and high reward. **Lawrence** noted that "there are only three types of enterprises left, and that includes government agencies, those who have been hacked, those who are about to be hacked and those that already have been hacked and don't know it yet." **Lawrence** asked what board members can and should be doing and if regulators have done a good enough job helping board members and what else could be done?

- **Clayton** suggested identifying "the constituencies that you most touch and most serve" and understanding how a cyber incident would affect this relationship. He noted that regulations are inconsistent because employees, customers and vendors are all cyber threats. By understanding that dynamic can add another aspect of preparedness.

Lawrence commented that he has historically been an advocate for companies to do a self-examination, "not only of where the vulnerabilities are in their systems and supply chains and vendor relationships, but also in identifying what assets do we have that might be attractive to these actors and why?" Boards are not just an operational arm of the organization but a means of guidance and support for management.

- Diversity is not discussed enough, noted **Clayton**. "We talk about diversity in skills, diversity in perspective, this is an area where we don't talk about diversity as much as we should."
- As well, there are different types of attacks, and understanding the motivation can help with resilience. Examples include disruptors, those looking to do damage or state sponsored entities. "That's everything from denial of service, to efforts to possibly corrupt your data, to… disinformation campaigns and getting between you and your various stakeholders," added **Lawrence**.
- **Clayton** advised to make an assessment of personal identifiable information and the board should ask if the data is necessary or if it should be digitized or removed.

Lawrence asked **Clayton** to explore the future of threats, to which he responded, "This sort of longer range threat is something that I think has more recently emerged and it shows why you need to continually update your thinking around these things." Observing a dysfunctional system currently in place, **Lawrence** commented there are a multitude of failures of disclosures, and suggested a need for a collaborative effort.

- **Clayton** agreed that success "requires coordination across not only intra-industry regulators, but then across various industries and

that type of coordination at the government level is nice to dream about, but it's never going to happen."

"Each industry has a different intersection with safety, security and quite frankly, our national interest and it's not one size fits all," commented **Lawrence**.

- Large scale financial institutions have two, three, or four regulators that need to sign off, as well as establishing some kind of relationship with DHS. But this is not the same for other sectors and "trying to do that on a multi-industry basis is just too complex a way to start," noted **Clayton**.

Lawrence noted that he has heard C-suites and board members asking why it takes a crisis for organizations to do anything.

- **Clayton** responded that "Proactive regulation is hard. Reactive regulation is a lot easier."
- It is hard in the climate of the system to be proactive, and "a backward looking enforcement-oriented approach to a systemic problem is much worse for investors, customers, etc., then a proactive forward looking approach."
- **Lawrence** and **Clayton** wrote an article published in the Wharton Business Review that claimed it may take a seismic event, like 9/11, in the cyber arena to force regulations and guidelines.

Lawrence further asked if "there is an opportunity here for corporate advocacy and how should one think about that to do it in the right way?"

- "The short answer is yes, of course and there should be," responded **Clayton**. Organizations need to ask how much money they are spending on security and with a more pronounced national consciousness can increase effectiveness.

There are parallels with the pandemic observed **Lawrence**, reflecting on the response by the financial sector when the government struggled to deal with the crisis. He hopes there are lessons learned that can be applied to cybersecurity.

- **Clayton** agreed "that [the] government and the private sector in this area of information technology and information sharing, particularly in the financial services area, did a great job in March and April of 2020 in the face of the pandemic." He argued it shows how reliant we have become on information technology, and "its resilience, its credibility, its certainty." Therefore investing in mitigating these risks is crucial.

Lawrence ended the interview by noting that there is a lot of information in our open and democratic society that can help inform about the evolution and nature of threats, so even if an organization is waiting for government regulation, they can and should do their own due diligence. ☐

Breakout Session: The Brave New World of Cybersecurity Compliance

Matthew Bey, Senior Stratfor Analyst at RANE, moderated a breakout session with **Colleen Valentine,** Head of Information Security Governance and Compliance at Nasdaq, and **Guillermo Christensen,** Washington DC Office Managing Partner at Ice Miller LLP, in this panel discussion: The Brave New World of Cybersecurity Compliance.

Bey began the session asking Colleen Valentine what are some of those challenges that she faced when she was developing the Nasdaq strategy around the issue of cybersecurity compliance.

- "Take a clear risk-based approach that's in line with the business priority and the business strategies," reflected Valentine, emphasizing the importance of partnerships on the business priorities and needs.

Bey then asked what are some of the challenges that **Guillermo Christensen** thinks people are working with when they deal with these compliance issues.

- Understanding the risk profile, and doing so with the assistance of legal counsel is paramount, said **Christensen.** "Some very big technological initiatives in companies often are headed in the wrong direction because we didn't start with that idea of what's at risk, what are the assets that we're concerned about? What's the business process?" There are frameworks in place to assess risk and ways to build those up with compliance in mind.

Continuing with a theme of best practices, **Bey** asked what carrying out a risk assessment would look like.

- **Christensen** suggested starting with the approach of small internal investigation, in "the same way that we inquire as to the root cause analysis of a problem, whether it be in a money laundering context or a cyber context." All the information gathered, and problems faced then need to be translated into a digestible context for the board to understand.

Bey then asked what **Valentine** would recommend to someone who is looking to get the board more involved in cyber security issues.

- Creating a dialogue with the identified key stakeholders is the most important, said **Valentine.** While "there's a level setting of the level of expertise both internally when it comes to the staff that are supporting the information security initiative…[having] an expert on the board that can really be a partner and help drive the dialogue [is crucial]." This means there is not one defined answer of best practices per industry or organization; "It depends on the nature of the business. It depends on the risk profile. It depends on the skillset of the board."
- Internal resources are important, but external resources help validate these findings, commented **Valentine.** This validation can "give a sense of assurance to the board as well, that [they] are on the right path when it comes to where [they're] going to be focusing the priorities."

A culture can really be a part of a cybersecurity strategy, noted Bey. He then asked **Christensen** to elaborate on what he means by culture.

- The strengths and weaknesses of systems all come down to human operators, commented **Christensen.** In terms of culture,

having a cyber security mindset has a bit of an element of paranoia to it. "When we do training, whether it's at a board level or for the employees or staff of a company, at the end of it, if the reaction is something along the lines of, "Boy, I didn't know we were doing all these things the wrong way, and now I'm really scared," we've done it the right way." A certain amount of skepticism is helpful to first and last lines of defense.

- **Christensen** advises automating aspects of the business process that intersect with cybersecurity, to lower the burden on employees and which can "reduce that risk from the human being, which is more difficult to mitigate."

Bey then asked **Valentine** how important she views people when it comes to getting compliance right where it needs to be.

- "The culture of security is really paramount to an organization. But behavior change is hard," noted **Valentine.** She spoke about when earlier in the pandemic, Twitter was hacked due to a user that did not question when they received a call requesting account verification. She suggested companies implement two factor authentication, where something as "simple as a phone call from a motivated attacker can[not] bypass that." Training is important to help individuals recognize the culture of security.
- **Valentine** also explained how at Nasdaq, they had a white hat hacker (someone who hacks to highlight vulnerabilities), and noted how eye opening the exercise was.
- **Christensen** added that security awareness training has to address the motivation of the exercise, and to ask questions like: "how is the cybersecurity program of the company making your life more difficult in trying to do the things you need to do to make the company successful?"

Bey then asked how boards should practice their incident response plans, citing increased importance with OFAC sanctioned cryptocurrency exchanges and/or in some cases ransomware affiliates.

- The best way is to practice it, **Christensen** said. "Like everything else, the amateurs practice to get it right. Professionals do it so that we never get it wrong." And the best way to practice is through tabletop exercises. It is good to be aware also that not one exercise fits all, and different size companies and different sectors will need different approaches.

Bey asked what some of the compliance changes and trends are happening inside and outside in the United States and Asia.

- In the United States, regulation is an overall trend, noted Valentine. In the EU they have TIBER, which is Threat Intelligence Based Ethical Red Teaming. Other trends are in "Data, privacy, data protection, data locality, and then also resiliency." While there has historically not been much cyber regulation, with changes internationally, it is only a matter of time for the US to follow.
- Asia market trends are focused on data privacy and locality and how they interplay. Companies need to question: "how are you ensuring that you either have the regulatory compliance in place and the security controls that can speak to what those requirements are," said **Valentine.**

"How would you recommend a company that's really trying to navigate those different competing and sometimes contradictory compliance requirements?" asked **Bey.**

- **Valentine** warned companies to not "operate in a vacuum. Understand your limitations and your expertise." Creating relationships with other companies that are complying in this space can provide guidance and act as a sounding board. Ultimately, not being in compliance is more risky than working in partnership with your competitors.

Bey then asked how the evolution from the regulators is evolving.

- Governments are playing catch up on creating regulations, said **Christensen.** This could be because they are not in the midst of cybersecurity risks constantly and the race to regulate technology is a losing battle, as technology will always move faster. **Christensen** explained that he is worried about GDPR as "an innovation stifling law. Europe has not advanced in many areas of innovation and data in part because of the concern around data privacy."

Bey asked **Valentine** what trends she is seeing in the States.

- "I think still the focus really is critical infrastructure and then also the government itself, and making sure that things are up to speed," said **Valentine.** She also has noticed Jen Easterly helping to rebrand the CISA to be more customer friendly.
- One challenge is the jargon and lack of a cyber or information security dictionary or consistently accessible lexicon. Being on the same page of what is an event or incident would be helpful across the States, observed **Valentine.**

Recently, there has been increased importance placed on cybersecurity because of the ransomware tax and events like SolarWinds. **Bey** asked the panelists what they think of some of the things that blindside a board or somebody in the C-suite when it comes to compliance issues and cyber security risks in the future.

- "I think the trend for larger enterprises that are able to spend more on cyber is we're headed towards more automated, integrated technology stack solutions to cybersecurity. We know we're going to have a much more effective cybersecurity solution when we have machine learning, and for lack of a better word, AI technology in those," responded **Christensen.**

Bey asked what small companies should do since they are often following behind other companies.

- Technology has evolved, and piling a solution on another when there is a weak foundation, such as in small companies, they will struggle to manage. **Christensen** noted that he doesn't "see phishing emails anymore with spelling mistakes or grammar mistakes. They're written better than some of the emails that I see from other lawyers. Why? Because the hackers are using Microsoft Word to write these… technology can be our enemy just as much as our friend."

"What are some of the things over the next five years that you are concerned about that could blindside different actors in the space?" asked **Bey.**

- **Valentine** echoed **Christensen's** sentiments, saying "I think regardless of the size, it's doing the basic things right. It has a culture of security. It's following your basic cyber hygiene. Making sure you're following the policies, the standards. It's fundamental."
- Companies will not be able to protect against a nation state attack, so focusing on preparation is key. Similarly, understanding what is happening with third parties, and knowing their touch points, who has access to that data, helps focus preparation and protect vulnerabilities.

The audience then asked how blockchain technology will influence the compliance space.

- Circling back to encryption, **Christensen** explained how blockchain allows for companies to keep track and keep corporate records of supply chains. "At its core, by being a distributed ledger, it allows us to keep track of information in more of an immutable form. If you're dealing with supply chain, if you're trying to keep track of information, it's helpful in that sense"

- **Valentine** added that a few years prior, "there was some mantra within financial services that was blockchain, not Bitcoin." More recently, companies like Walmart used blockchain to track their food supply shipments, showing a development in the technology and the application.
- **Christensen** added that an area he wants to "see more of a technological approach is the process of pushing out your requirements to your third parties, having them come back," with confirmation. By automating the process and taking people out of the equation, compliance can become more streamlined and efficient.

Bey asked how the pandemic has altered the compliance when it comes to monitoring supply chains.

- There is a need to focus on the right risk in that respect, responded **Christensen.** "For most companies, the supply chain risk is not because the Russians have infiltrated a major IT services company. It's because you have people that are sharing your systems or your data, and they have zero security."

Bey then asked the panelists to give their concluding thoughts.

- "I would just echo that cyber security compliance or information security compliance isn't going to be done in a week. It's not going to be done in a year. This is a marathon. It's a constantly changing landscape when it comes to both the threat actors and the regulations. For mature organizations, it's really critical to resource the function correctly to make sure you have the subject matter experts who can understand where the risks are, what the compliance requirements are, and how you're going to address that within the organization. Whether it's through policy, processes, technology. And to continue to be able to mature that capability within the organization," said **Valentine.**
- Cybersecurity compliance "should be a boring, normal problem that every company is dealing with. If we are treating it as an exceptional one, we're not doing the normal things that we should be doing," concluded **Christensen.** ☐

Breakout Session:
Getting the Board and Cyber Leadership on the Same Page

It often seems like board directors and cybersecurity professionals speak a different language, but clear communication between the CISO and the board is critical given the board's public disclosure requirements.

In this session, Getting the Board and Cyber Leadership on the Same Page, **Rick Borden**, Counsel, Corporate & Financial Services Department and Cybersecurity and Privacy at Wilkie Farr & Gallagher LLP, moderates a discussion with **Joan Conley,** Senior Advisor on Corporate Governance and ESG Programs at Nasdaq, and **Tim Murphy,** President & CEO, Consortium Networks.

The discussion covered ways to establish open communications between the CISO and the board and best practices for creating a common framework that enables CISOs to effectively communicate material cyber risk to directors and gives CISOs a better understanding of the board's disclosure requirements.

Rick Borden, the moderator, started the discussion by acknowledging the difference between management obligations to the board and the board obligations. He then asked the participants about the different roles and responsibilities and how they think the conversations are taking place.

- **Joan Conley** identified that while there is a difference, there needs to be an educational partnership between the two. By offering tabletop exercises, companies can distinguish where the roles and responsibilities lie between the board and staff.

Borden asked **Tim Murphy** what his view of the board's role in cybersecurity for the company was.

- Boards usually look at risk, and cybersecurity is just a new type of risk, said **Murphy**. He agreed with **Conley** that education is essential to help translate information on these types of risks.

In 2018, the SEC put out a guidance saying that cybersecurity risk is a financial risk. **Borden** asked the panelists what risk their companies face, what it means, and how best can boards bridge these gaps.

- **Murphy** suggested creating an appendix so members can understand the jargon which will help to focus on questions both sides or a risk organization can understand. These include: "What are our biggest threats? What visibility do we have? What are we doing about it? What are our biggest vulnerabilities?" It is also important to develop metrics to help quantify the size and scope of threats.

Borden asked panelists how to create that connectivity.

- **Conley** explained how she, "in concert with the general council, created an acronym dictionary that was focused on all of the language that the CISO and the CTO were speaking." This resource, along with an education program, was then translated into a dashboard which organized threats by category. This is then assessed monthly to rate threats and continues to evolve. The dashboard is in coordination with an audit committee and the board to develop tabletop exercises.

- "You have to identify, we have to protect, we have to detect, we have to respond and then we have to recover," said **Murphy**. This works alongside a maturity model.

- If you don't understand something, if you don't know what it actually means it's important to ask, emphasizes **Borden**.

- **Murphy** suggested starting at the foundation of the company and asking how the board will mature the organization.

- Meeting the entire CISO team is one of the "most impactful" parts of onboarding, **Conley** experienced, and recommended others request team tours.

- The board should also encourage companies to establish a relationship with regulators prior to a possible cyberattack, said **Murphy**.

There are different types of cyber risk that are not just attacks, noted **Borden**, such as data leaks. Companies may think of cyber security in terms of external threats, but internal errors, even by third parties, should be prepared for and included in cyber leadership agendas.

- Efforts to ensure cyber security within a company is a team effort, emphasized **Murphy**. While "there's a separation between management and what the board's responsible for, a board can provide a lot of guidance" to differentiate internal failures or external attacks.

- **Conley** reiterated the importance of table top exercises to help a corporation prepare for all possible scenarios. This should be multiple run throughs, one within the staff and one with the board, and other line leaders, such as head of risk, security, and IT. Attacks can "not only can it happen in cyber, but [they] can be something natural."

Borden asked **Conley** to explain what a tabletop is and how it plays out in reality.

- In a tabletop exercise, **Conley** explained staff "are given a set of circumstances. [They] have to respond, [each person] has a role and knows what to do. [Staff] then as part of the table, there's an incident and there's a plan for as part of this directory and dictionary, which [they] all keep. There's audit, there's the CISO, there's cyber, there's legal, there's risk. [They] have somebody playing board members. [They] have somebody playing external advisors or external advisors and external consultants with [them]. But [staff] go through this scenario and then do a debrief."

- In the debrief, employees discuss what went well and what went wrong, and try to identify what areas need improvement or if roles are missing.

- "The goal of a tabletop is to create a scenario where all of the key decision makers and their teams are in roles where they would be, if there was a real life situation. The exercise then becomes so increasingly valuable on the debrief side. The debrief can be about three times as long as the actual exercise and the takeaways and the improvements are then communicated with the whole team and become part of the team goals."

Borden asked the panelists to end the session by sharing how individuals can better communicate with the senior management board on cybersecurity.

- Both panelists agreed that education is foundational to increase communication between directors and executive team.

- **Conley** also suggested being proactive and asking questions, while **Murphy** suggested treating cyber risk like other risks and improving situational awareness by doing exercise to help show vulnerabilities before attacks happen. ☐

Breakout Session:
Surviving a Cyberattack — Best Practices for Board Response

Every company remains vulnerable to a cyberattack, and the question is not if it will happen but when. How a company responds can make the difference between a manageable incident and a reputational crisis.

In this session, *Surviving a Cyberattack: Best Practices for Board Response,* **Judy Germano**, Founding Member of GermanoLawLLC, moderated a discussion with **Art Coviello**, Venture Partner at Rally Ventures and Board Member at FireEye, and **Kevin Zerrusen**, Managing Director, Cybersecurity Advisory Services at EY. The discussion covered the board's role in incident response and best practices for building organizational resilience as well as balancing the board's oversight role with its fiduciary duty.

It is sometimes unclear how to balance the line between board oversight and management running a company, observed **Germano**. She identified many questions that are asked, such as: "How should those communication structures work? How involved and invested should the board be? And what are the right roles for board members? What questions should they be asking?" **Germano** first asked **Coviello** to speak about his experience with the SolarWinds hack and if there are key takeaways.

- Coviello spoke about the FireEye hack and how by focusing on the potential danger the attack presented to their customers, and in coordination with an active board, they were able respond to the attack

- He cited their "tremendous track record of being able to respond to attacks, and they basically played their own handbook on their own attack. They were the first company to recognize that it was SolarWinds behind the attack and their disclosure of what happened to them was instrumental in bringing down all the information around SolarWinds."

Germano agreed with **Coviello's** observation that there has been a lot of development and growth in the regulatory landscape. **Zerrusen** added that these need to be taken into consideration.

- "While some companies have additional regulatory responsibilities, like financial services companies or those in the health sector in particular, all publicly traded companies have a responsibility to notify of any kind of material event to the organization," noted **Zerrusen**.

- While he believes regulators are becoming increasingly strict on notification requirements, organizations need to also be aware that "individuals in the company are not trading stock during that period of time, lest somebody pursue you for insider trading." Timing can be everything.

Germano asked **Coviello** if in years that he has been in an advisory role, if the board's responsibility has changed over the years or is it the same responsibility perhaps with higher stakes?

- **Coviello** said the board should always do the right thing, not just in terms of regulations, but also for the customers and larger community.

When you're a board member and you have a fiduciary duty to the company, and by starting from

the position of, "let's do the right thing" is great, but in retrospect, sometimes it's easier to know what that is, said **Germano**. She then asked if the panelists have any tips or advice on asserting what is the right thing.

- **Coviello** noted that every situation is different, since sometimes one may not have the right information, and with disclosure requirements.

- **Zerrusen** agreed, adding that investigations take time, but when attacks happen, regulations assert protocol on disclosure timelines. He suggested "contact the FBI and local authorities, inform the regulators, file the proper forms and so on and so forth. Essentially do the right thing." By following steps to be transparent, organizations can minimize damage from a reputational risk perspective and legal exposure. He also suggested bringing in "anybody that can help you manage the incident to limit the liability and the damage that will occur."

- By doing the right thing, your stock can even increase, **Coviello** suggested, citing the FireEye example. "When they disclosed that the stock not only bounced back, it even went higher than before the incident occurred. It just shows you that stock prices will bounce back, the world will not come to an end. Compounding the problem by not doing the right thing is when you run into trouble."

Having discussions ahead of time with the board is essential, noted **Germano**, who then asked what these conversations mean in terms of the regulatory context and the table talk exercises.

- Boards should be involved in table top exercise, said **Coviello**, adding "there's no substitute for them because it's like exercising a muscle."

- **Zerrusen** observed that attacks do not happen on a 9-5 schedule, so companies need to have an incident response plan that includes scenarios such as ransomware pay, to assist those making the decisions in real time. These simulations should also include thought process exercises to understand decision making, and how to answer questions like: "How would we talk to our customers? How would we talk to the press? How would we engage with law enforcement? How would we engage with regulators? What would we need in terms of help and support, and are those individuals or entities available to help us?"

Being proactive and knowing the right players are very valuable, summarized **Germano**. She then observes that a lot of companies struggle with, "When should we tell our board? How much detail should we tell our board? How often should we address cybersecurity issues to the board generally and in a crisis, and is it to the full board or the audit committee?"

- "You need to separate the two roles a board can play here. One is, can they add any value to the process or the incident? The other is in their fiduciary and governance role. You have to evaluate the level of seriousness as to when to inform the board and engage them.," suggested **Coviello**. Additionally, while early notification is important, understanding the select individuals to receive this information is paramount.

Germano asked what the panelists' perspectives were on whether there should be cybersecurity experts on boards or not.

- **Zerrusen** did not think that that's an absolute requirement due to his experience with boards that had a basic understanding of cybersecurity and the importance of patching and fixing vulnerabilities. "Maybe that's just a natural evolution of where the boards are today, but I've been impressed with all the boards that I've had the opportunity to chat with."

- **Coviello** disagreed to some extent, believing expertise on the board was fundamental. He cites how every organization has been digitally transformed, so "If, as a requirement of every board, there's a financial expert, how can you possibly have a board that doesn't have a technology expert on it?"

Germano asked in terms of oversight, if there are particular benchmarks or questions that the board should be asking management to determine if management sufficiently has its fingers in on the cybersecurity issues.

- Cybersecurity risk is not binary, so to stay ahead of hackers requires constant assessment but also an understanding of the level of risk a company is willing to accept, said **Coviello**. If everything was static, you'd have a chance to stay ahead of the hackers, but we're expanding the attack surface all the time. "The data, which is the currency in our digital world, the applications on which the data run and how you protect them. Then the infrastructure on which the applications run and the data is created. Further, what is the backup and recovery plan? What is your response?"

- "The board has visibility, and with that comes accountability and responsibility" added **Zerrusen**. By sharing pertinent information, being transparent and open with the board can develop a key relationship within the organization.

Germano asked the panelists to discuss M&A experiences in relation to due diligence, based on their backgrounds and what suggestions they have for best practices.

- **Coviello** noted how when one acquires a company, they also acquire all the vulnerabilities that come along with the organization. By reviewing their cybersecurity practices "before the acquisition is done and before you expose them to your own corporate network would be serious due diligence malpractice. Clearly that would be job number one. In terms of inquiry, clearly you need to understand what potential problems might exist."

- Not disclosing cyber risk or breaches is a large red flag, added **Zerrusen**. "If you discover through your due diligence that the company hasn't disclosed properly on cybersecurity-related matters, you should think seriously about whether you want to complete that deal."

Germano asked the panelists to give their closing thoughts on best practices for board response in a cyber attack.

- **Coviello** said while you hope nothing will happen, you still must "Prepare, prepare, prepare, there's no substitute for that."

- Also recommending preparation, **Zerrusen** added, "Have a plan, make sure the plan is documented, and practice and test it and you'll reap the rewards for that." ☐

Panel Discussion:
Incorporating Cyber Intelligence Into Your Board

Discussion of practical steps on how the board can improve situational awareness of key issues that may impact the company, with implications for board composition. Focus on how the board can integrate cyber risk analysis and scenario planning into their oversight and decision-making process.

Denny Watson, Executive Director of RANE, moderated a discussion with **Terry Roberts**, Founder and CEO of Whitehawk, **Dianna Burley**, Vice Provost for Research at American University, and **John Ford**, Cyber Strategist at IronNet Cybersecurity, in this panel discussion: Incorporating CyberIntelligence into your Board.

Watson began the webinar by focusing the discussion on how organizations can best incorporate cyber intelligence into their board discussions, and asked the panel what are the next steps.

- **Roberts** noted today it is an imperative for boards to be on top of their cyber threat landscape, cyber risk, and cyber response planning — recommending these be discussed on a quarterly basis at a minimum.

- **Burley** added it is about positioning oneself in the near term and future to pivot from "thinking about the security posture in isolation, to thinking about it in the context of everything else that's happening, and that you're focusing on, both within your enterprise, and also contextually in the environment." By taking a holistic approach, what she calls "forward leaning" can help an organization stay on top of how the threat environment is constantly evolving.

- Boards need to play a more active role in hiring security leaders within a company, added **Ford**. "When it comes to hiring the security leader, this organization, they need to be educated enough to take an active role, and understand, do they have the right team? Do they have the right leadership? Do they have the right strategy?" As well, board members should push for better self education.

Watson then asked the panelists to talk about the changing landscape, what has changed or is changing specifically with regard to cyber intelligence.

- **Ford** observed that today's threat actors, "whether nation state or not, they're very brazen, very audacious type attacks" and have a great support system. It is a viable opportunity because it is easy to get into, as being a threat actor is low risk and has low competition. In the United States, which is very networked, it is easy to execute attacks at a high velocity and volume. **Ford** cited "the amount of threat actors, non-nation states, grows 25% year over year."

- **Roberts** noted that criminals of all types have just moved online. Like **Ford**, she noted the attraction of the job is due to "ease of entry, non-attribution, [it's] hard to prosecute, relatively low cost, and you can even buy a mercenary to bring onto your team" All economies are targets, as actors could be hacktivists (with a cause) or engaged in espionage.

- **Burley** added that "criminals don't have to have a great success rate." With cyber-attacks, they only need one or two "wins" to be successful, making a very strong motivator for staying in this game. Companies then need to consider how they spend their time and

attention and must think critically about the motivation an actor may have to help reduce their vulnerabilities.

Given the changing landscape, **Watson** then asked: "how do boards get better information? Or the information that they need from inside of the organization? What are the right, best questions, boards should be asking? And how do boards help the organization become more sophisticated, and better able to meet, or mitigate growing cyber threats?"

- "It is not a cybersecurity problem, it's a business risk," said **Roberts**. All businesses operating in the digital age, their dependents and adversaries, operation and interaction all are risks. Organizations need to put in place priorities to mitigate those risks.

- Companies have a lot of moving parts, and security is a big component, so boards need to get their arms around that first, noted **Ford**. As well, it is foolish to think attacks can be prevented to a certain degree. Instead, boards should ask how prepared the business is when the event occurs. **Ford** uses an analogy of how in Florida, people don't try to prevent hurricanes, because they can't, and instead focus on how to respond when they do happen and what they can do before to prepare to mitigate the fall out. In addition, boards need to ask: "Have you done tabletop exercise based upon the scenarios that are identified against our company? What was the outcome of that? What do we need to do as a response to that? Is this team mature enough to handle that type of an attack? Who are our business partners that we have lined up that we need to call in in the event of an attack?"

Watson then turned to **Burley**, highlighting the previous discussion where she noted the importance of having an integrated conversation not only just around cyber issues. **Watson** asked **Burley** to add to this.

- Businesses cannot be successful without integrating every part of the enterprise, as assessing risk is not an isolated activity, said **Burley**. This needs to be constant, "and the cadence has to be the cadence that makes the most sense for your enterprise, for your sector, for your environment." Organizations need to "get into the mindset of continuously assessing, and re-assessing risk, continuously working through tabletops, continuously engaging with different parts of the organization to ensure that we are continuously aware of, and comfortable with the risk appetite under which we're operating."

Watson then asked how the board can have confidence in what they're being told from inside the organization and if there is a role for external voices.

- This can be done by having an independent external source to validate information, said **Ford**. " Validation externally is the most important thing, as well as the education to the board to understand what is being delivered to the board members."

- In board meetings there is often not a lot of time for engagement to ask questions that need to be asked, basic or advanced, noted **Burley**. These need to be addressed.

- **Roberts** added, "I actually think a lot of the cyber regulatory environment has been burdensome, as opposed to enabling,." She agreed that external audits are helpful.

Continuing off the conversation of audits, **Watson** asked where companies find third parties to complete audits, and if organizations can use the same firm that does their financial audits or their cyber provider.

- **Ford** suggests getting an independent firm to audit, not because of conflict of interest, but

to gain additional opinions and perspectives. **Burley** agreed, citing the benefit of fresh eyes.

- **Roberts** also agreed, and added her concern "that the big guys also aren't as up to date on innovation, whereas the mid-tier tend to be trying new things, reaching out."

Watson then asked: "What kind of organizational structure is optimal, and why? Where should the board focus first? Cyber intelligence? Cyber threat strategy? Execution and responsibility, or accountability? Is it the CSO, the CRO, the CSO, the CEO, someone else?"

- Stressing the need to be forward leading, understanding security in constantly changing context and as an integrated component of everything a business does is critical, noted **Burley**. "It is not an IT issue," she said.

- There has become a trend of "elevating the business risk landscape to a chief risk officer, because it should focus on how your business operates, [and asking] what your business objectives are?," **Roberts** added. She also agreed that this should not be a technical issue.

- **Ford** agreed that "the worst place for it is IT [as] they have very competing goals. CIOs are there, and compensated to move business objectives forward through the use of technology. Sometimes that is not in alignment with the risk landscape, or the threat landscape depending upon the organization's current structure."

In the U.S. there have been several pieces of legislation being considered in congress, at the federal level, multiple states have passed their own data breach, data governance, data privacy laws and regulations. As well as a new executive order from the Biden administration, noted **Watson**. She then asked: "Is there a way that companies can take advantage of what is happening in the legislation, regulation environment? What are the limitations? And how can they best navigate as that moves forward?"

- With every executive order that comes out, it shows that at a government level, they're paying attention to this and they understand the problem, said **Ford**. He stressed the need to "proactively, and anonymously share actionable attack intelligence in real time with the government, such that the government can be responsive."

- Expectations need to be calibrated, added **Burley**, in addition to building trust between sectors. "Part of having that trust is having realistic, and shared expectations of what we will be able to accomplish, and when, because if we have different ideas of where we'll end up, and when we'll end there."

- Intrinsically, industry will never trust government and government will never share everything with industry, responded **Roberts**. Digital issues are still being approached with industrial age thinking, and those involved (from leadership to government to academia) are not technically informed on the realm of the possible. "So, when we talk about resilience, smart response, accountability, it has to be with the enablement of these technologies and capabilities, which we need both government and industry to fully leverage."

- **Ford** added that organizations need to stop defending in isolation, as it isn't successful; "adversaries [that] work together are successful."

- **Watson** then asked the panelists to end the discussion with some closing comments.

- "I think board members with outside help really need to push hard on the right metrics that will give them the right information so that they can adequately guide the organization. Don't be afraid to say, 'This means nothing to me,'" said **Ford**. "I'm hoping that boards are

curious enough to really seek the right information externally to validate what they're hearing internally."

- "I would add that [businesses] need to lean forward, and to really think about what is happening in the future, not even today, but where are we trying to go? How is the threat environment evolving? How are we positioned, and how can we be positioned in order to understand that?" added **Burley**. "It can be basic sessions that just give you the language, the jargon, the terminology, the basic concepts. But get it, and get it before the CSO, before the independent auditor comes in, and then get it again afterwards, so that you can contextualize what you've heard, and make sense of what you've heard. That's really critical."

- "Engage in your sector and engage with the government on what is the regulatory environment," said **Roberts**. She stressed using tabletop exercises with both the board and executive team participating,"because it will level the playing field for you." ☐

Closing Keynote Interview: Cyber Warfare — Nation State Actors and the Threat to Critical Infrastructure

David Lawrence, RANE Founder and Chief Collaborative Officer, interviewed **Jeh Johnson**, Partner at Paul, Weiss, Rifkind, Wharton & Garrison and Former U.S. Secretary of Homeland Security, in this Closing Keynote Interview: Cyber warfare: Nation state actors and the threat to critical infrastructure.

Lawrence began the interview by introducing Jeh Johnson and highlighting a speech he would be giving to the Atlantic Council on December 13, 2021.

- **Johnson** explained that the topic of the speech is on cyber attacks on critical infrastructure in the United States, specifically energy infrastructure, utilities, and the power grid. "I make a point of saying that in my judgment cyberspace is the new 21st century battle space. It's the new war zone, and we have to treat it as such." He also explained that cyber bad actors are most often non-state actors.

Lawrence built upon the analogy of modern warfare and asked why the cooperation of companies is essential and how board members should be thinking of the governance of their organizations.

- Public-private partnerships are essential, as between 50%-80% of critical infrastructure is in the private sector, explained **Johnson**. Some companies also take part in cybersecurity compliance through their own fiduciary duty. Spear phishing is a devastating attack that can be prevented through awareness training.

- He also encouraged minimum cyber security standards at the federal level, noting "we regulate maritime safety, aviation security, road safety, why not cybersecurity?"

Companies are not in a position to fight back but are positioned to become victims, observed Lawrence. Yet, there is an expectation for cooperation with the government in terms of threats and disclosure of potential breaches. Johnson suggested companies make cybersecurity report updates a routine agenda for board meetings. As well, these should be explained to boards in plain English so more can understand where the shortcomings and vulnerabilities lie.

Lawrence then explained how simplicity is not easy, even when it is incumbent upon the board in working with management to make sure the executive team has access to information and expertise. He also noted that companies cannot manage the threat to zero but can position themselves to be protected and resilient.

- **Johnson** explained organizations need to understand the nature of the enemy, who they are and who the targets are. He discussed his experience with a Chinese hack, where the government denied a cyber attack by the nation-state but blamed an individual, to which **Johnson** found: "governments have cut outs in the private sector that used to work for their state security apparatus, that are now out there in the private sector, who do their dirty work for them. It gives them a degree of deniability. And some of these groups have dual objectives. Sometimes they respond to the state's request to do their dirty work, and sometimes they're in it for themselves."

- Therefore the goals and nature of the enemy are ambiguous. "Sometimes the enemy is a state actor, sometimes it's a private actor who is functioning with the government looking the other way, or sometimes it's somebody who's one degree removed. Now, that presents a complicated threat picture, which is why I think we need to regard in some instances, non-state actors as dangerous as state actors," said Johnson.

- He also explained that any organization with large amounts of data can be a target, such as a hospital, hotel, airline, or even university.

Observing that Congress is passing opportunities to create standards within critical infrastructure that companies could follow, **Lawrence** asked Johnson's thoughts on this and any guidance of where the world is headed and what board members should do.

- **Johnson** noted that there have been many attempts to enact cybersecurity standards most of which have failed. He cited the Cybersecurity Act of 2012 and a clause added to the National Defense Authorization Act which would require reporting requirements of cyber incidents. For big organizations, they're not the ones experts worry about, said **Johnson**. "We worry about those in the supply chain, we worry about new entrants into critical infrastructure. We worry about the mom and pop operation to the extent it still exists.

Lawrence then asked how we summon up political will, and, until then, what should board members be thinking about.

- There is a lot that can be done in terms of defense, said Johnson. "Certain attacks are bound to be effective, which is why when you're dealing with a nation state actor, and even some non-state actors, you have to make the bad behavior cost prohibitive. You have to create sufficient deterrence so that it is simply not worth it for the bad actor to engage in the bad behavior anymore."

- **Johnson** also believes it is incumbent upon those with a voice in the private sector to continually pressure the government to call out bad actors. But, "it's up to the government to provide sufficient deterrence and protect us by way of offense. And those in critical infrastructure need to continually remind the US government of that."

- Companies often feel that if they come forward that an attack has occured, they will be shamed, stock prices will be affected and investigations will start. Lawrence asked how companies disclose and who they call for other guidance.

- There is a "cyber 911" that the public is not aware of, **Johnson** noted, but currently, for threat response you call the FBI or CISA, often chosen by where the organization's personal relationships lie.

- **Johnson** acknowledged companies' fear of reporting, but reassured listeners that confidentiality is of the utmost importance. This can only be promoted through trust, which is a continuous work in progress and is beneficial in the long run. When companies report, "If [they're] the victim [they] benefit from understanding the larger picture, [they] benefit from understanding 10 other entities got attacked the same way and this is what they did." The government can only share this if an organization is willing to disclose the incident.

Lawrence reiterated the shame companies feel being a main component of why they may not disclose, to which **Johnson** hammered away at the fact that no one is "impervious or immune" to these attacks. "The shame comes when the victim delays reporting it. You think, what were you thinking? You knew about this in July, and now it's December you're telling me? That's where the

shame comes, the delay. And I think we therefore have to re-incentivize in terms of how we think about this kind of thing."

Circling back to the analogy that cyber threats and attacks are a new battleground of war, **Lawrence** highlighted the board's need to understand various state actors and organized crime groups in this realm. He also observed this as an opportunity for boards "not only to think through where they're at risk and what can be done, and to think in common sense simple terms, but also to be advocates." **Johnson** repeated this sentiment, saying, "I personally believe that conventional state on state kinetic warfare is becoming a thing of the past. And that the principal battlefield is cyber."

Lawrence ended the webinar by quoting himself when saying to someone senior at Goldman Sachs, "When the big boys go bowling, you don't want to be a pin." And companies are unfortunately the pins. ☐

Speaker Profiles

Matthew Bey, Senior Stratfor Analyst, RANE

Matthew Bey is Senior Stratfor Analyst at RANE where he covers a wide range of topics in international relations. Matthew has focused heavily on geopolitical, political, economic, and security issues in the Middle East and Africa. Matthew also covers several international topics relating to global governance, technology, trade, and the oil and gas industry. Matthew has a bachelor's degree in mathematics from Texas Lutheran University and a masters degree in mathematics from the University of Texas at Austin. You can follow him on Twitter at @Matthew_Bey.

Diana Burley, Vice Provost for Research, American University

Dr. Diana L. Burley is a proven leader able to establish and maintain strategic partnerships, manage broad portfolios, and achieve high quality results. She is an award-winning global cybersecurity expert with nearly 25 years of experience leading multi-institutional, cross-sector teams to drive education, research and strategic innovation. She is a dynamic industry thought leader who identifies holistic approaches to strategic challenges, designs and implements robust workforce development programs, and advocates for a diverse cybersecurity/high-tech workforce and an equitable global cyber community.

Diana is currently Vice Provost for Research at American University (AU) where she is also a Professor of Public Administration and Policy and Professor of Information Technology & Analytics. As the university's chief research officer, she is responsible for establishing the strategic vision and executing against the research and revenue targets set by the board while also overseeing the university-wide research enterprise, developing the research brand, and supporting faculty led scholarship across all disciplines.

Richard M. Borden, Counsel, Corporate & Financial Services Department and Cybersecurity and Privacy, Wilkie Farr & Gallagher LLP

Richard M. Borden is counsel in the Corporate & Financial Services Department and Cybersecurity and Privacy practice group where he focuses on intersecting areas such as technology transactions, cybersecurity and privacy risk management, Fintech and Insurtech.Rick is at the forefront of cybersecurity and privacy issues, advising on big data governance and the Internet of Things, cybersecurity risk management, and technology sourcing and transactions. Rick translates the often complicated language of technology, cybersecurity, privacy, risk and compliance to assure that it's understood from both a legal and business perspective. His experience on both the customer and vendor side of matters enables him to advise general counsel, C-Suite executives and boards of directors on how to understand potential risks and how to respond should they suffer an incident. Rick also interfaces with technology departments, advising them on how technology tools and programs may expose companies to risk.

Guillermo Christensen, Partner, Data Security and Privacy and White Collar Defense Groups, Ice Miller LLP

Guillermo Christensen is a partner in Ice Miller's Data Privacy and Security and White Collar Defense Groups. Guillermo combines his experience as an attorney, a former CIA intelligence officer and a diplomat with the U.S. Department of

State to shape and inform the advice he provides to clients on various enterprise risks involving cybersecurity and national security law. His cybersecurity experience ranges from conducting information security risk assessments that take a "whole of company" approach to managing responses to security incidents and breaches, including those where a nation-state or insider threat may be involved. Guillermo also counsels clients in managing national security reviews through the Committee on Foreign Investment in the United States (CFIUS), particularly those involving high-technology and critical infrastructure sectors.

Jay Clayton, Sr Policy Advisor & Of Counsel, Sullivan & Cromwell, Former Chairman of the U.S. Securities and Exchange Commission

Jay Clayton, who recently served as the Chairman of the U.S. Securities and Exchange Commission, is a Senior Policy Advisor and Of Counsel to Sullivan & Cromwell. Mr. Clayton's practice centers on advising institutions, board of directors and individuals on governance, markets and regulatory matters, particularly where multidisciplinary advice and practical experience are valued. As Chairman of the SEC from May 2017 to December 2020, Mr. Clayton focused on modernizing the regulation and oversight of our equity and fixed income markets, concentrating on the interests of long-term investors. In addition, under his leadership, the women and men of the SEC addressed various market developments and emerging risks, including the 2020 COVID-19 economic shock, the digitization of securities and other assets, the Brexit and LIBOR transitions, and various cybersecurity matters. Prior to Mr. Clayton's government service, he spent over 20 years at Sullivan & Cromwell where he was a member of the management committee, co-managing partner of the General Practice Group and co-head of the Cybersecurity Group.

Joan Conley, Senior Advisor on Corporate Governance and ESG Programs

In February 2021, Joan was elected to the board of EJF Acquisition Corp., where she also serves as Chair of the Nominating and Corporate Governance Committee. In July 2021, Joan was elected to the board of Tigo Energy, a private company providing smart module technology for the solar industry. Joan also serves on the Advisory Board of Harvestly.co, an entrepreneurial initiative started by Cal Poly students focused on feeding the community by connecting local farmers and consumers in San Luis Obispo, Calif. Additionally, Joan is a member of Executive Women on Boards (EWOB). On Dec. 31, 2020, Joan retired from her role as the Senior Vice President and Corporate Secretary of Nasdaq, where she was responsible for the Nasdaq Global Corporate Governance Program and the Nasdaq Global Ethics and Corporate Compliance Program as well as the Nasdaq Educational Foundation, following 19 years at Nasdaq and 19 years at NASD, now FINRA. In her former role at Nasdaq, Joan also served as a Managing Director of the Nasdaq Educational Foundation from 1994 - 2020 and a founding board member of the Nasdaq Entrepreneurial Center from 2014 - 2020.

Arthur W. Coviello, Jr., Venture Partner, Rally Ventures, Board Member at Mandiant

Arthur has been an active investor and advisor in the technology industry, guiding a number of startups as a private investor and in his roles as a Venture Partner at Rally Ventures, as an advisor to ClearSky Security Fund, and as a Senior Advisor to Blackstone's Tactical Opportunities Group. From January 2001 Art served as President and CEO of RSA and following RSA's acquisition by EMC (for $2.1B) as an Executive Vice President of EMC and head of its Security Division. Art has been a central

figure within the information security industry for more than 25 years. Under his leadership, he built RSA Conference into the most respected, vendor agnostic event in cybersecurity. He is frequently a featured presenter at conferences and forums around the world, and he has played key roles in several national cybersecurity initiatives.

John Ford, Vice President, Cybersecurity Strategist, IronNet Cybersecurity

John Ford is a compliance, IT, information security, and operations executive, specializing in designing, building and transforming regulated organizations. Mr. Ford serves as Cyber Strategist with IronNet Cybersecurity, a global cybersecurity firm that is revolutionizing how enterprises, industries, and governments secure their networks through collective cyber defense networks. In his role, Mr. Ford assists senior executives and government agencies across the United States, United Kingdom, Europe, Asia and Middle East in crafting and implementing cyber security strategies and programs. Mr. Ford is a member of the board of directors of the Cloud Security Alliance and an advisory committee member at the University of South Florida - Cybersecurity for Executive Education. Prior to joining IronNet, Mr. Ford served as CISO and head of the Cybersecurity Center of Excellence at ConnectWise. Before joining ConnectWise, Mr. Ford founded and led the Sienna Group. The firm focused on protecting organizations most sensitive data, and bringing visibility to their security posture up to the Board/CXO level. As a former CISO and CCO, Ford's unique perspective served as a foundation to Sienna's practical approach to providing services to its clients.

Judith H. Germano, Founding Member, GermanoLawLLC

Judith Germano is a nationally recognized leader of cybersecurity governance and privacy issues, and served more than a decade as a federal prosecutor. In addition to founding GermanoLawLLC, Judi also is a Distinguished Fellow at the New York University Center for Cybersecurity and an Adjunct Professor at NYU School of Law.

GermanoLawLLC, founded by Judith Germano, specializes in cybersecurity, privacy, securities and other financial fraud and regulatory-compliance matters, providing companies and individuals with legal and strategic counsel and representation.

Jeh Johnson, Partner, Paul, Weiss, Rifikind, Wharton & Garrison, Former US Secretary of Homeland Security

A partner in the Litigation Department, Jeh Johnson has had a distinguished career combining private law practice at Paul, Weiss and senior-level public service, including three Senate-confirmed presidential appointments. In public life, he served as Secretary of Homeland Security (2013-2017), General Counsel of the Department of Defense (2009-2012), General Counsel of the Department of the Air Force (1998-2001) and as an Assistant United States Attorney for the Southern District of New York (1989-1991). In private practice, Secretary Johnson is an experienced litigator and trial lawyer, and a Fellow in the American College of Trial Lawyers. Since returning to Paul, Weiss in 2017, Secretary Johnson also advises clients, including high-tech companies and government contractors, on the legal aspects of cybersecurity, national security, data privacy, government contracting, crisis management, high-stakes litigation and regulatory matters. Secretary Johnson is currently a member of the board of directors of Lockheed Martin and U.S. Steel and is a trustee of Columbia University. In June 2020 the Chief Judge of New York appointed Secretary Johnson to assess equal justice in the state court system. After a four-month investigation, Secretary Johnson issued a 100-page public report recommending a number of changes, all of which the Chief Judge said would be adopted.

Byron Loflin, Global Head of Board Engagement, Nasdaq

Byron Loflin is Global Head of Board Engagement at Nasdaq, where he leads board assessments and boardroom training for Nasdaq Governance Solutions. He is the founder and former CEO of the Center for Board Excellence (CBE) – acquired by Nasdaq in 2019 – and is architect of CBE's unique board assessment and advisory platform. Byron is recognized in the governance community for developing unique products that address board dynamics, corporate culture, accountability and performance. His experience and expertise are in the design and administration of assessments and advising board chairs, boards, committees, directors and executive management in a full range of corporate governance matters including strategic alignment, best practices, board refreshment, diversity, structures and corporate planning. He and his team have performed several hundred third-party board, committee, peer and CEO self-assessments for organizations of all structures and sizes.

David Lawrence, Founder & Chief Collaborative Officer, RANE

David Lawrence is the Founder and Chief Collaborative Officer of RANE. He previously served for 20 years as Associate General Counsel and Managing Director at Goldman Sachs. His role as the global head of the Business Intelligence Group covered a wide range of legal, regulatory, diligence, and transactional responsibilities. David led the development of Wall Street's first design and implementation of controls and technology to safeguard against money-laundering, illicit finance, terrorism financing, foreign corrupt practices, and violations of economic sanctions. In 2014, David received the FBI Director's Award for his efforts in combating international terrorism.Prior to Goldman Sachs, David served for 10 years as an Assistant US Attorney, in the Southern District of New York. He served as the Deputy Chief of the Criminal Division, Chief of the Public Corruption and General Crimes Units, and as the office's first Chief Ethics Officer.

Tim Murphy, President & CEO, Consortium Networks; former Deputy Director, FBI

With 30 years of public and private sector experience—primarily in the Federal Bureau of Investigation—Timothy P. Murphy is a recognized leader in the global law enforcement, intelligence, and business communities.Mr. Murphy maintains close ties to the law enforcement and intelligence communities and is frequently consulted for his expertise in global cyber, counterterrorism, intelligence, criminal, and security issues and is a guest lecturer at colleges and universities on these issues. He is frequently called upon to speak on these topics in the media. He is member of the Police Executive Research Forum, the International Association of Chiefs of Police (IACP), the Department of State Overseas Security Advisory Council (OSAC), Deputy Co-Chairman of the FBI/DHS Domestic Security Alliance Council (DSAC), the FBI Agents Association, and the FBI National Academy Associates. He is also member of the Advisory Board of two cyber-security companies, on the Board of Directors for a data analytics company, and The Foundation Board of Directors for Ferris State University.

Terry Roberts, Founder & CEO, Whitehawk

Terry Roberts has established the first Cybersecurity Online Exchange - enabling all businesses (especially mid- sized and small companies) to have continuous online access to tailored learning, smart buying, and connections to the best products, services, insights, and trends industry wide. Previously, Terry was the TASC Vice President for Cyber Engineering and Analytics, running all Cyber/IT, Financial, and Business Analytics cross cutting, innovative technical services. Prior to TASC, Terry was the Executive Director of the Carnegie Mellon, Software Engineering Institute, leading the technical body of work for the entire US Interagency, with a special focus on leverag-

ing and transitioning commercial innovation and acquisition excellence to government programs and capabilities, and establishing the Emerging Technologies Center and Cyber Intelligence Consortium.

Colleen Valentine, Head of Information Security Governance and Compliance, Nasdaq

Colleen Valentine is the Head of Information Security Governance and Compliance, reporting to Nasdaq's Chief Information Security Officer. Colleen is responsible for the "softer", people side of Information Security, including policies and standards, IT control library, metrics and board reporting, alignment to industry standards, cyber security regulatory compliance, global security awareness Programs, program communications, and the Nasdaq Cyber Service Center which manages the security due diligence requests received from clients.

Denny Watson, Executive Director, RANE

Prior to joining RANE, Denny spent 27 years as an analyst with the Central Intelligence Agency. In addition to creating and leading several large, innovative analytic programs at CIA, Denny served as the President's Daily Briefer to Vice President Gore and Secretary of Defense Rumsfeld, and also served on the Senate Armed Services Committee staff for Senator Nunn. In recent years, Denny has developed big data analytics solutions that address emerging risks in the public and private sectors.

Kevin Zerrusen, Managing Director, Cybersecurity Advisory Services, EY

Kevin provides cybersecurity services and develops new product offerings for the financial services sector. Prior to EY, he served as the Senior Advisor for Cybersecurity Policy to the Chairman of the SEC and spent five years at a global investment bank. He also worked at the CIA, where he led the Agency's Cyber Center. He has an MBA from Syracuse University and a BA from the University of Dayton. ☐

info@ranenetwork.com

1-844-786-RANE

www.ranenetwork.com

RANE

Risk Assistance Network + Exchange