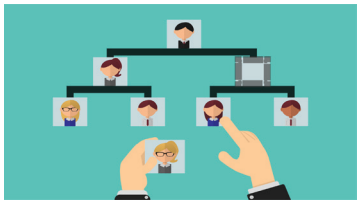

Fourth-Party Cyber Risk: Securing the Endpoints of Your Business Ecosystem

FEATURED EXPERTS

Earl Crane, Owner, Earl Crane LLC; Former Director of Cybersecurity Policy, NSC

Craig Moss, Executive Vice President, Ethisphere

Kamil Shields, Special Counsel, Sullivan & Cromwell LLP

MODERATOR

Patrick Sheehan, President & CEO, **Fellsway Group**

The modern, digital economy is more interconnected than ever before, and companies today rely on a network of partners and third parties to efficiently deliver their services. But the expanded role of third parties also exposes them to additional cyber risk. More than half of the cyber breaches in the United States can be traced back to third parties, according to a recent study. Attackers look for the path of least resistance: They know that companies focus their attention on their own defenses, so they gain access by compromising a key vendor or a supplier to a key vendor. Companies spend a lot of time and money on internal security and protecting critical information, but all of those efforts are wasted if the data is then shared with a less secure third or fourth party, sometimes without the company's knowledge. In a recent RANE webinar, a panel of experts examined best practices for creating a dynamic cyber risk management strategy to help actively manage the endpoints in the vendor supply chain. Highlights of the conversation follow.

Moderator **Patrick Sheehan** kicked off the webinar by asking, "When we think about third parties and fourth parties, where do organizations need to start?"

Craig Moss said that he would first assess and prioritize the risks and take a risk-based approach. "If you have hundreds or thousands or tens of thousands of third parties that you're dealing with, you really can't spend the same amount of time and energy on all of them. You have to find a way to segment them into groups," he said.

- "Then based on that segmentation, apply the right level and type of contractual or monitoring or other types of controls to be able to mitigate the risk that they pose."
- Once business partners are evaluated into tiers, the next step is to think about how to effectively engage with third parties and "the understanding that each of the third parties could have dozens of fourth parties that they're dealing with on their behalf."
- Next, there needs to be an internal program to manage the third-party risk, **Moss** said. That requires "cross-functional collaboration," which requires an organization "to pull together the different functional areas to collaborate around the idea of how do we manage risk in our third parties."
- **Moss** reminded that cybersecurity "is a people process and technology issue."

"We see that HR can play a critical role in effectively reducing cyber risk and really improving cyber readiness in the organization and then cascading it to third and fourth parties." — Craig Moss

Moss added that such broad collaboration requires involvement from legal, from enterprise risk management, and from the IT department or the CISO and "whoever has the third-party relationship." "In a lot of cases because you're dealing with your employees managing a third party, HR should be involved in this also," he said. "We see that HR can play a critical role in effectively reducing cyber risk and really improving cyber readiness in the organization and then cascading it to third and fourth parties."

TRUST BUT VERIFY

Moss shared an anecdote about a "cyber maturity" assessment he performed of a mid-sized company that supplied several large defense contractors. "They said … 'Usually, we just got a checklist, and we know that in that checklist that we need to say yes to somewhere between 70 and 85 percent of the questions. If we're lower than 70, it raises a red flag. If we're above 85 percent yes on the checklist, people want verifications. We've gone through this 40 or 50 times with different big defense companies and we know that we should be between 70 and 85 percent.' I said, 'Has anybody ever checked to see how you answer and if you actually are accurate?' He said, 'No. Nobody has ever checked.'" **Moss** said the example illustrates how organizations need to think about what happens pre- and post-contract. "Due diligence up front is critical, but then there should be some kind of monitoring in the relationship," he said. "That gets back to the risk-based approach because you can't monitor everybody equally with the same degree of rigor. It's really a balancing act."

Kamil Shields noted the presence of Know Your Customer (KYC) documentation requirements in the financial space. "You're aware that some customers might pose risk for monitoring that," she added. "I think the same could be said here where you have to know your supplier, know who you're dealing with." Risky customers should result in ongoing monitoring, **Shields** said. "The same kind of practices, the same sort of cross collaboration we see in the AML space I think can also be present here."

Earl Crane added that in regulated environments, like the financial sector and the federal sector, regulators expect better management of third-party risk, as well as around the suppliers to your third parties. Increased sophistication from examiners and customers mean "that they want to see that their suppliers have a handle on their own supply chain as well," he added.

INSIGHTS ON AUTOMATION

Responding to a question of resourcing, **Crane** noted that there is a clear trend toward the cloud. "There's been a lot of great efforts both in the government and the big commercial space to try to get to a better level of control standardization," he said.

- "In the commercial space, you have the Cloud Security Alliance and their STAR (Security Trust Assurance and Risk) framework," **Crane** said, noting that it encompasses " everything from a self-attestation to a third-party assessment of your activities as a cloud service provider."

- On the government side, there is the federal grant program, "which has been making some incredible progress as they align the way government does its compute and outsourcing to third parties and the way that they look at that to standardize those processes," he added.

- **Crane** also noted the National Institute of Science and Technology (NIST) Critical Infrastructure Framework includes "a whole section that calls out the needs for supply-chain risk management. There's an increasing number of tools that provide elements of

automation and orchestration when you're looking at that third and fourth party risk management."

DEGREES OF RISK ASSESSMENT

Crane offered a way to differentiate between third- and fourth-party risk management. "An analogy that I like is: I'm a dad with three young kids. We have a daycare. When we put our kids out, when we drop them off of daycare, we're outsourcing, watching the kids for the day to a third party." The risk management in this instance includes meeting the teachers, checking their certifications and accreditations. "The fourth-party risk would be the contractors they hire, the maintenance crew, the building that they're in, bus drivers — and some daycares will have swim coaches and gymnastics coaches that will come in to teach," **Crane** said. "What's the background check on those providers? That's your fourth-party risk management. When you start thinking of it from that context, you realize how hard it is, hard to the parent to begin with, how hard it is to keep an eye on the risk that you're exposed to."

Sheehan asked for examples of how organizations can mitigate — or at least account for — some "some of those risks that they don't control as it relates to fourth parties."

"To say it simply, you can't control what you don't know," **Crane** replied. "The goal of identifying what it is that you might not even be aware of is a way to start to bring that into your sphere of influence, your domain of control." Yet fourth-party risk is "a completely new way of thinking about a risk-management process: It means that we're exposed to new loss scenarios and new risk scenarios." That means being able to think through a risk-based approach, he added. "We also need to think through new risk scenarios that we've created that they might not have been exposed to. Unfortunately, humans are bad at coming up with new dynamic scenarios that are different than what they've seen in the past."

Crane added a critical element. "To try to identify future losses before they happen is an important mechanism to try to start figuring out what's in that sphere of influence, what's outside that sphere of influence — and trying to get your arms around those areas that you previously didn't know about so you can start to control that risk."

THE FOURTH-PARTY BALANCING ACT

Moss noted a challenge in an organization's attempts to grasp fourth-party risk. "If we look at it from a practical business standpoint, a lot of third parties do not want you to know all the fourth parties involved," he said. "There are business reasons that they want to keep that veil there. The idea of unauthorized subcontracting is really prevalent in the supply chain. If you look at other types of compliance risk, unauthorized subcontracting is one of the biggest risk areas."

Moss added that it was important to "cascade your expectations from the third party to the fourth party and try to gain visibility," a feat that he acknowledged was challenging. "The idea that the third party is going to open up all the fourth parties to you is not really accurate from a practical business standpoint," he added, calling it a juggling act.

While there are inherent challenges in vetting fourth parties, **Moss** said that cybersecurity was somewhat different. "With cybersecurity, I feel that there's an inherent desire to be more transparent about what's going on and that companies realize that everybody really is in it together," he said.

Shields agreed. "That's absolutely true because — also to an earlier point — the fact is that if there is a breach and that breach occurs, either your company or the third party and when you're working with law enforcement, or you're dealing with a regulator to address that, or some sort of a prosecutor, they're going to wonder, 'What did you know? What kind of visibility did you have?' … So really getting, understanding that and having a transparent process just at the end is beneficial for all.

RANE

THE GROWTH OF TECHNOLOGICAL CHALLENGES

Technology itself is a contributing factor to fourth-party risk, **Crane** said. The growth of web-based application programming interfaces (APIs) and JavaScript Object Notation (JSON) feeds that help power cloud-based products has resulted in greater system integration with outside entities. That present a challenge many organizations — and their legal departments — might not have considered, **Crane** said. "And so maintaining control on that for fourth-party risk management is critical." **Sheehan** added, "If we're aware that certain entities are using fourth parties, maybe there's some contractual vehicles that we can leverage to enforce and control the uncontrollable risk."

Moss noted the value of the NIST cybersecurity framework. "We see increasing adoption of the NIST Cybersecurity Framework as a way for companies to evaluate the maturity of their third parties' controls. Of course, then you cascade that to the fourth party." While not everyone needs to be "at the same maturity level," it's important to identify "third parties who have either critical system access or are accessing critical data," he said. "Then from there, to be able to assign a realistic maturity level to them."

Moss said that the most effective approach with third parties is "a shared learning," rather than a traditional, pass-fail audit. "We've been doing a lot of programs like that where we're going in to work with third parties on behalf of large companies. We start by saying to the third party, 'We want to understand where you are today,' and then we have resources and tools to try to help you drive improvement," he said. Rather than having a pass/fail audit approach, we start with maturity targets. "You then can raise the targets over time to help them actually get into the continual-improvement cycle."

'CYBERSECURITY RISK APPETITE'

Crane offered the concept of "cybersecurity risk appetite," saying, "A risk appetite is briefly the amount of risk an organization is willing to take to accomplish its goals." He noted that the term originally came from the Dodd-Frank Act and investment risk "but has now been well-adapted in the cybersecurity community because we're all about taking risk and risk management in the cybersecurity world as well." Yet measurement is also important, he added. "Then by putting those metrics behind it, we can start measuring the amount of risk that we're taking relative to our appetite."

"One of the concepts that we walk through with the students who are usually CSOs and aspiring CSOs is the DIKW information model — that's Data Information Knowledge and Wisdom." — Earl Crane

Crane also noted that one of the classes he teaches is advanced cyber-risk management. "One of the concepts that we walk through with the students who are usually CSOs and aspiring CSOs is the DIKW information model — that's Data Information Knowledge and Wisdom." Briefly, he described it as a type of KPI or KRI but with risk indicators. "When you look at information, it's one of those vulnerabilities and how important are they," he said. "When you look at knowledge, it's those vulnerabilities on systems that are the most critical and the ones that could impact my business the most. Then when you get to wisdom is: What will happen if I don't do that."

MEASURING IMPACT

Shields raised a related concern. "What examples have we seen where people have really thought about what is going to be the impact of a breach transfusion to the reputation of my company?"

Crane noted a "misperception" years ago "that a reputational risk would impact shareholder value" with share price as a useful metric. "What we learned after breaches like Target was that the share price recovered, and that if the organization still provides a good product, that people will continue to patronize it, even looking past prior cyber incidents," he said. **Crane**

added that two outcomes are now more likely: "executive consequences," or a C-suite sacking, and a longer-term impact on reputation. "One of the reasons crisis communication consultants have so much opportunity out there is that you can do a lot to repair reputation after you've had that reputational impact."

Moss emphasized the difference "between maturity metrics and performance metrics." Using the example of phishing, he said that it's important to understand whether a program to counter that risk includes repeatable processes, whether training is routine and continually updated, and whether training is extended to contractors. "All of those are things where you can measure program maturity," he said. "Performance metrics would just be what percent of people click on a phishing email."

Sheehan asked how companies think proactively about crisis management, noting that a recent Ponemon study found that the average cost of a breach is $3.8 million.

"Once a company becomes aware of a breach, they need to be working with law enforcement," **Shields** said. "I think that that is true for a Fortune 100 or financial services company or even a very small company." While many organizations might be wary of working with law enforcement, it's "incredibly important" to do so, she added, partly because of the forensic experience they bring to an investigation.

Shields also emphasized the importance of complying with reporting obligations, even as she acknowledged the "tension" of reputational risk. "I do think that you need to make your customers and your employees aware that potentially their personal identifying information is out there," she said. "At least some of the prosecutions that I was involved in, people are selling PII. They are literally selling account numbers, names, and they're doing it on the cheap." Understanding the consequences of a breach, she added, makes it easier to work with law enforcement to stop it. Then, organizations must consider how to prevent it from happening again.

Moss said he liked the idea of an incident response plan. "In looking at a third party or certainly a fourth party, that's really one of the things that you need to make sure they have in place," he said. "If something happens, do they know what to do. Do their employees know what to do?"

Sheehan said that during panels, he often asks how many security practitioners or those in the executive ranks have incident response plans or some sort of tabletop exercise. "You get 50 to 60 percent of them to raise their hands because not everybody is all that participant," he said. "Then I ask of that subsection, how many people are doing it with folks outside of IT? It's significantly less. I say, 'Well, where's legal? Where's crisis communications?' … We're digging into a lot of things that brings us back to program maturity that we just need to be aware of." **Sheehan** added that cyber teams and IT "are only a piece of the puzzle." "You need to have documented plans," he said. "You don't want to be dusting your intendent response plans off during a breach. That doesn't help anybody."

"You need to have documented plans. You don't want to be dusting your intendent response plans off during a breach. That doesn't help anybody." — Patrick Sheehan

Shields said that when thinking about incident response plans, it's important to include a broad array of people. "It's not just IT," she said. "It's legal. It's compliance. It's HR. All of the different facets that are going to be affected by a breach should be involved."

REACHING OUT TO LAW ENFORCEMENT

Sheehan posed the question of whether organizations are reachinging out to authorities proactively, *before* an incident.

"Because in so many areas of civil or criminal liability, people are thinking about a risk-based approach to avoid their real consequences."
— Kamil Shields

"No, definitely not," **Shields** said, adding that she couldn't understand why the target of a breach wouldn't look to forge a relationship. "It is law enforcement's job here to assist," she added. "You're the victim." **Shields** also said that a number of US Attorneys' offices are working more closely with companies in their jurisdiction. "What I would encourage people on the line to do is to reach out to know who they're dealing with," she added. "You are the entity whose trust has been violated, where there has been a breach of the law, not only breach of your infrastructure. You can be working with law enforcement."

Noting her background as a former prosecutor, **Shields** said that law enforcement can assist in putting "on hold whatever systems are in place," which will allow for a more thorough investigation. "The concern is the longer you wait, the more people that are involved before you are involving law enforcement, it might be that emails haven't been saved, that various things have been deleted. All of those are going to be important threats for the investigation."

FINAL THOUGHTS

Moss touched upon the idea of leverage and control in a business relationship.

- **Moss** noted that leverage and control can change pre-contract and post-contract. "It shifts based on the nature of the relationship that you have with them from a business standpoint."

- He also stressed the idea of cross-functional collaboration. Where an IT department might call out a third party for weaknesses, the operations side can see the same partner as a critical supplier. "Those are the types of things where that cross-functional collaboration is absolutely critical, so that you're conveying a consistent, clear message to third parties and then cascading that to fourth parties about your expectations."

Crane highlighted the idea of evolving how organizations think about cyber risk — away from "a checklist model" and toward a "risk-based model."

- He offered employment background checks as an analogy. "Anyone who's had a background check done knows that you are asked to provide references, but those are not the references that the investigator is interested in asking," **Crane** said.

- Instead, HR seeks assessments from disinterested fourth parties. "That's the same type of challenge we're dealing with in risk management is our fourth parties don't have the same type of vested interest in protecting our information as our third party unless we've made that explicit in contractual requirements."

Shields emphasized the importance of a risk-based approach.

- "It's the approach these companies are aware of," she said. "Because in so many areas of civil or criminal liability, people are thinking about a risk-based approach to avoid their real consequences."

- Early steps, too, are critical. "So many companies think about this already," **Shields** said. "They think about AML issues. They think about bribery issues. They think about all of these kinds of things that are baked into what a company does. I think using that perspective for cybersecurity will be very valuable."

RELATED READING

Promoting Convergence and Collaboration to Combat Cyber and Physical Risks

Improve Cyber Hygiene to Prevent Business Email Compromises

RANE Expert Spotlight: Building a Digital Cocoon Against Cyber Threats

The RANE Spotlight Series: Effective Vendor Screening and Other Third-Party Due Diligence

ABOUT THE EXPERTS

Earl Crane, Owner, Earl Crane LLC; Former Director of Cybersecurity Policy, NSC

Dr. Earl Crane is a cybersecurity executive and trusted advisor to public and private sector organizations, helping them to manage their strategy, risk, and cybersecurity programs. He is a prominent cybersecurity veteran, having worked at early security startups, the White House National Security Council, Department of Homeland Security, the financial sector, and other Fortune 100s, and founded Emergynt, a digital risk management platform based on his Ph.D. research. He is an adjunct professor at Carnegie Mellon where he has taught cybersecurity to graduate students and executives since 2002 and is a Cybersecurity Fellow at the University of Texas at Austin Strauss Center. He holds a Ph.D. from George Washington University, and a Master of Information System Management and B.S. in mechanical engineering from Carnegie Mellon University.

Craig Moss, Executive Vice President, Ethisphere

Craig Moss is a leading expert on using management systems to improve compliance performance within companies and across supply chains. At Ethisphere, Moss is responsible for developing and delivering Ethisphere's maturity assessment service designed to help companies and their supply chain companies measure and improve their programs for cybersecurity, protection of intellectual property and anti-corruption. He has designed and led numerous programs helping Fortune 500 companies around the world to implement management systems to reduce supply chain risk and improve performance. Moss is the Director-Content & Tools at the Cyber Readiness Institute, an organization focused on helping small and mid-sized businesses in the value chain improve their cyber readiness. He is a Director of the Digital Supply Chain Institute, where he developed a transformation catalyst program, featuring a unique new data trading framework. Moss is also Chairman of the Licensing Executives Society committee for developing a global standard for IP Protection in the Supply Chain. He has developed guides on implementing management systems to improve compliance for organizations including World Bank Group's International Finance Corporation and the United Nations.

Kamil Shields, Special Counsel, Sullivan & Cromwell LLP

Kamil Shields is a special counsel in the Firm's Litigation Group. Her practice focuses on investigations and regulatory enforcement proceedings involving cybercrime matters, public corruption, and bank and wire fraud. Shields rejoined the Firm in 2019 from the United States Attorney's Office for the District of Columbia, where she served as an Assistant United States Attorney in both the Cyber Crime and Fraud and Public Corruption sections. In her capacity as an Assistant United States Attorney, Shields served as lead prosecutor in 13 jury trials, investigated and indicted dozens of cases, drafted and argued procedural and substantive motions, worked with expert witnesses, and coordinated with victims of fraud and other crimes.

Patrick Sheehan, President & CEO, Fellsway Group

Patrick Sheehan is an internationally experienced business leader with a superior record of creating and building successful and high performing organizations. He possesses a solid understanding of global business trends, sales and marketing fundamentals, team building and business development practices. Sheehan is a self-driven individual with a proven track record of helping organizations of all sizes achieve desired growth objectives, while successfully mitigating cyber and technology risk. As President and CEO of the Fellsway Group, Sheehan's purpose is to help business leaders and key stakeholders protect their organizations from the myriad of threats facing all companies, while securely enabling business growth.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.