Vetting Your Vendors: Third-Party Cyber Risk Assessment

In partnership with opus

Featured Experts

Charlie Bradley, Chief Technical Officer; **John Kerr**, Vice President, Technical Counterintelligence, Commercial Solutions; Federal Data Systems/NOBUS Technical Counter Intelligence

Dov Goldman, VP of Innovation and Alliances, Opus

Laura Louthan, Founder, Angel Cybersecurity

Sean Weppner, Managing Director for Operations, Nisos Group

The Target Breach — the 2013 attack on the US retail chain's point-of-sale systems — remains the gold standard in how not to allow third-party access to an organization's critical networks. Yet nearly four years after the breach took place, securing enterprise networks against intrusion from malicious actors who gained access via a vendor or partner remains an ongoing effort amid increased vulnerabilities and expanding access points. To help organizations guard against third-party cyber risk, RANE recently spoke with a number of experts in the field. Key takeaways from the discussions follow.

HIGHLIGHTS

- **Enlist external expertise**: Red-team exercises can uncover previously unknown vulnerabilities, including with mobile devices, IoT and the Cloud.
- **Understand the scope**: Organizations should determine what exactly they want from an assessment; not every single contractor can be thoroughly screened, if at all.
- **Consider the cost**: Inaction (possibly leading to a serious breach) could be more expensive in the long-term.
- **Perform strong due diligence**: This should include talking to HR at a third party to see how they screen new people, as well as performing continuous monitoring (both technical and performance-based).
- **Get it in writing**: Contracts should include detailed third-party responsibilities, including how much they need to vet their own partners and the minimum security steps they must take in order to gain access to your systems.
- **Follow the principle of "least privilege"**: Properly segregating data so that contractors and partners have no more access than they absolutely require will help your company avoid becoming the next Target.
- **Look ahead**: Third-party data security compliance involves more than check-the-box policies.

GAUGING THE THREAT

Laura Louthan recalls being "stunned" at the findings from one of her first red-team exercises, which exposed vulnerabilities that "never would've crossed my mind." Today, the threat potential can be multiplied by "a hundred different applications" used within an enterprise — and their weak points may not always be obvious.

Dov Goldman notes hearing from an organization in the wake of the WannaCry ransomware attack that had upgraded all its Microsoft Windows systems, and as a result believed they were inoculated from the malware. "Then they start getting notifications that their third parties were being hit," he adds.

"The weakness in organizations is the same as it was 30 years ago, which is the people," **John Kerr** says. Ransomware is an example of how malicious actors exploit such a vulnerability — and presents an ongoing challenge for enterprises seeking to mitigate the internal threat. "A lot of that still starts at trying to identify a vulnerable individual who's likely to click a phishing attempt."

Weppner points out that readiness doesn't always correlate to the size of an enterprise. Smaller, forward-looking companies might see the value in training personnel against such threats as spearphishing campaigns. "In other cases, with multibillion-dollar multinationals, network segmentation is completely flat," he says. "We're regularly able to take control of entire corporate networks within a couple of days."

SETTING THE SCOPE

"The C-suite should consider, what's the objective?" **Charlie Bradley** says. "What do they really want to get from an assessment? Some just want to be compliant." A complete gamut of security testing "could benefit them possibly more than they can imagine," he adds, but organizations have to establish an end goal, and at some level, "they should prepare to hear things they don't really want to hear."

Louthan says it comes down to tried and true practices. "It's due diligence. That's really all it is." Any third party receiving data should be held to the same standards as internal organizations. "I don't think people necessarily think of data movement in that same way." At the same time, she adds, "I think you have to understand not every contractor is going to get looked at." The focus should thus be prioritized on the third parties that have access to systems, networks and physical spaces that could result in greatest exposure.

"What are your regulators going to ask you? You have to think about the outputs before you think about the inputs," **Goldman** says. Narrowing the scope, however, is also critical. "Some of the banks I talk to have 4,000 appraisers. Do you send them each a thousand-page questionnaire?"

Kerr notes that third-party risk assessments have changed mostly in the breadth they require once mobile, IoT and e-mail are factored in. "I do believe that an effective risk assessment these days needs to include an understanding of the breadth of the environment and how companies are protecting their information on mobile devices."

Weppner views the task as minimizing risk, rather than trying to eliminate it. "It's not about building a big wall," he says. "It's about compartmentalizing before (malicious

actors are) in. When there is an incident, it's about figuring out who they are, what are they doing and why, and eliminating their foothold from the system."

JUSTIFYING COSTS AND EFFORTS

"The other thing missing in a lot of programs is a focus on marketing within the organization. You should be asking: Why are we doing this? If the answer is 'regulators,' that's not good enough." A robust third-party program will include continuous monitoring, which carries benefits that might not be immediately apparent. "Think about the value in knowing that a vendor is slipping. Or that a vendor's procedures for perimeter security are failing," **Goldman** says. "You want to know how that organization is doing, and you might want to revisit that relationship and convey your concerns. How can you convey those concerns if you don't have the facts?"

Weppner says that while costs are understandably a concern, that's only part of the picture. "We try to pivot that and make it more of a profit center — generating value instead of just encumbering costs," he says. Beyond meeting privacy-related requirements in such legislation as the EU's General Data Protection Regulation (GDPR), which is important for board members and the C-suite, organizations need to understand "that they will be held responsible for not just the trust of their employees but their customers too."

When the price tag of a cyber risk assessment is raised, **Louthan** says that the alternative, a potentially much costlier breach, has to be kept in mind. "It takes up so much time, potentially an enormous amount of money. It can be really punishing on a small organization with 100,000 customers," Louthan adds. "That's 100,000 who are going to be posting on social media," not to mention legal fees, forensic fees, etc. "It's time wasted." While it may not be a "fun" budget item to consider, the benefit is clear: As Louthan puts it. "It may be expensive to find out, but it's better to know your weak areas."

BEST PRACTICES: WHO TO TALK TO, WHAT TO ASK...

Beyond the technical aspects of an assessment, examining key roles should be part of the process, "meeting different folks at different levels throughout the organization," **Kerr** advises. "One of the main departments we speak to is HR (to ask questions such as), 'What does that onboarding process look like? What kind of security awareness is there?'" The frequency of reassessments should be understood, as well as the process and procedures, he argues.

"Continuous monitoring should also mean you're getting data from multiple sources that will tell you about something wrong in between the annual reviews," **Goldman** says. Of course, monitoring can be greatly assisted by a technology component, such as the abillity to detect vulnerabilities like an open port on a perimeter device. "The other side of the equation is performance monitoring, which can be a very useful leading indicator," he adds. "If your vendor is beginning to respond more slowly, if they miss delivery dates, if they don't complete tasks," it could be a sign of heightened risk, Goldman notes. In some industries, slipping performance is "a good leading indicator of financial problems or management issues."

"Following frameworks that have been set by the industry are good starting points," **Weppner** says. "There's not a lot of recreating the wheel that you should do. Where risk lies as a business should inform where your next steps should be and creating

those tailored best practices." The National Institute of Standards and Technology (NIST) control framework remains "a great cookbook for securing your internal infrastructure," **Goldman** points out, yet it falls on other organizations to be diligent. "Are your vendors doing that? That's where the WannaCry ransomware hit a lot of people."

"It's good to let somebody loose in your organization, and let them see what they can find," **Louthan** adds. "That might not be the report you share with your customers, but it's important to help prioritize what you'll be working on, whether it's turning off a setting that allows everybody access to your data or some other significant risk mitigation. There's a lot of leverage associated with that."

"You want to operate from the principle of 'least privilege,'" **Goldman** advises. "If Target had simply applied the principle of least privilege to their vendor population, and properly blocked access to data, we wouldn't have heard so much news about the famous Target breach." Remember that they were breached via "a third party acting as a vector, unwittingly providing access into a network that connected to a (point-of-sale) system."

GETTING IT IN WRITING

Louthan acknowledges that enterprises can't go much further than third parties when assessing cyber risk "because you don't really have a direct relationship with the subcontractor's subcontractor." For that reason, contracts would benefit from "strong language" that requires third parties to vet their own business partners.

"We push a lot of our organizations that we work with to set a baseline or standard that each third party must comply with," **Kerr** notes, adding that this can be achieved via service-level agreements (SLAs). "It's a three-, four-page document that says, 'Here's the standard of security. Here's the baseline, or the bare minimum from a security perspective that you're going to have to meet to gain access or connection.'"

WIDENING THE SAFETY NET: CLOUD, BYOD, IoT, AI ...

Bradley offers a caveat when looking at technology solutions. "Boards and C-suites are going to hear a lot of promises from machine learning, AI, and it has great potential, but it's not a silver bullet," he says. "The adversary adapts."

"Organizations have to think through locking down mobile devices so people can't use their own device on a corporate email network," **Goldman** says. "These are good, basic best practices. You need to think about them in new areas."

Kerr says that best practices include requiring third parties answer a series of questions if they allow personal access to enterprise data: "Does the consent to monitor carry over to this personal device? What are the procedures for when an individual leaves the organization? Can the company wipe the device to ensure that no company information resides on the device?"

Louthan says that IoT devices sometimes get overlooked from a security standpoint. "Nobody really likes a black box on their network, but when it's a fridge, nobody thinks about it as much," she notes. "But is it on your internal network?" When it comes to cloud-computing services, Louthan notes that major cloud services have security tools

available that have to be purchased and set up properly. “Cloud is complicated because cloud can be done really, really well — but the default settings are not geared toward security.”

“Companies should be willing to take steps such as requiring a VPN,” **Weppner** recommends. “When it relates to IoT, it’s a huge opportunity space and problem space, as there really is no security standard.” He adds that organizations are now also honing their tools on the industrial Internet of things. “IIoT is the big elephant in the room,” Weppner says. “It’s something that we talk about, but companies tend not to test those systems.” Taking down insecure IIoT enterprise systems can be costly and time-consuming. “Strong protocols can help,” Weppner says, especially considering that “the lifespan of Internet-connected devices is not necessarily beyond a year or two, and you can have orphaned devices still connected to a network.” Being able to quantify those devices is important, he notes; “Businesses need to be especially wary when it comes to early adoption and should not take that lightly.”

LOOKING TO THE FUTURE

Goldman notes that there is a regulatory move “pushing you to cover a larger portion of your third parties, especially given the focus on tier 1 or ‘critical’ vendors within most financial services organizations.” Yet organizations need to keep a focus on maintaining their third-party cyber diligence, as opposed to a check-the-box approach. Regulations, Goldman adds, “are telling you, ‘If that’s all you’re doing, we’re going to ding you.’”

Louthan, for her part, says she’s not one of those professionals who worry about the next biggest threat. “Half of breaches are old vulnerabilities,” Louthan says. “It’s not crazy, new stuff that’s bringing people to their knees. It’s old stuff that people didn’t mitigate.”

“There still has yet to be death of a company due to a cyber incident,” **Weppner** argues, noting that the vendor blamed for the Target breach is still in business. But that could soon change, he cautions: “In the next year, we’ll see the next event where a company ceases to exist.”

ABOUT THE EXPERTS

Charlie Bradley, Chief Technical Officer, Federal Data Systems/NOBUS Technical Counter Intelligence
Charlie Bradley most recently served as Technical Director of the Technology Directorate for the NSA, where he was responsible for the agency's global operational network. Previous technical leadership assignments included the Office of Target Reconnaissance and Concealed Systems Division, where he spent significant time forward-deployed in support of the agency's mission.

John Kerr, Vice President, Technical Counterintelligence, Commercial Solutions, Federal Data Systems/NOBUS Technical Counter Intelligence
John Kerr is an experienced information technology executive (CISSP, CISM) with strong leadership skills. He previously served as the head of Global Identity and Access Management Delivery and Operations for a large telecommunications company, where he directed the technical support teams of four data centers and three Security/Network Operations Centers. Kerr has supported an array of government customers and was responsible for engineering and architecture of a multi-government targeting and analysis solution. He has developed global security policy/procedures for various customers and has established audit programs for three data centers located in Maryland, England, and Australia. He holds degrees in computer science and mathematics.

Dov Goldman, Vice President, Innovation and Alliances, Opus
Dov Goldman is an expert in regulatory compliance and third party information security, and is responsible for the Opus' Third Party Management (3PM) Information Security strategy. Goldman advocates a strategic, controls-driven approach to managing third party cyber risk, based on his ongoing work with CISOs and IT vendor risk professionals, and speaks regularly on how organizations can enhance and streamline their third party InfoSec risk strategy.

Laura Louthan, Founder, Angel Cybersecurity
Laura Louthan had more than 15 years of experience in IT architecture and infrastructure before moving in the past six years into responsibilities directing information security risk and compliance initiatives for global corporations. Managing risk while improving security in complex international environments, Louthan has experience fully designing and implementing secure solutions in support of business objectives.

Sean Weppner, Managing Director for Operations, Nisos Group
Sean Weppner is a leading expert in technology innovation in cybersecurity and intelligence analytics platforms. He has spent the better part of the last 10 years within the Defense and Intelligence Communities designing and building systems for the ingest, storage, analysis, and visualization of cyber and intelligence data, at scale, of which, the last two were focused on Deep Learning applications. At Nisos Group, Weppner is responsible for Technical Partnerships, Client Engagement, Product Development, and Media Outreach.

ABOUT OPUS

Opus is a leading provider of innovative compliance and risk management solutions combining flexible SaaS platforms with unparalleled data solutions, helping clients identify and mitigate external risks quickly and efficiently. Formed through the $500M partnership of Doug Bergeron, Chairman of Opus, and leading Private Equity Firm GTCR, Opus is changing the landscape of risk management.

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.