



Third-Party Risk:

'You've Been Breached - How Can I Trust You?'

SolarWinds, Kaseya and the next big supply chain security breach – they all have the same point in common: Their attackers seek to breach the largest number of enterprises possible solely via the third-party technology they use. As a potential target, you may detect warning signs even before your infected partner does. You can notify your partner and cut off access, but what then? How does your partner subsequently validate that it's clean and give you confidence to restore access? How do you protect your critical systems and data in a new extended world where every supply chain relationship needs to constantly be verified before it's trusted?

In this panel discussion, **Jamie Walsh**, Senior Director of Product Marketing at SAI360; **Richard Rushing**, CISO at Motorola Mobility; and **Jo Stewart-Rattray**, CSO at Silver Chain Group; take a deep dive inside third-party risk and discuss:

- What to do when you detect your partner's breach;
- How to cut off access and protect your systems and data with minimal business disruption;
- When it is appropriate to restore access and how to conduct effective ongoing monitoring.



Jamie Walsh / Senior Director of Product Marketing at SAI360

Walsh is the senior director of product marketing at SAI360. He has over 15 years of experience in governance, risk and compliance - or GRC. His specialties include risk management, business continuity and regulatory compliance.



Richard Rushing / SCISO at Motorola Mobility

Rushing is the chief information security officer for Motorola Mobility. He leads the security effort by developing an international team to tackle the emerging threats of mobile devices, targeted attacks and cybercrime. He has organized, developed and deployed practices, tools and techniques to protect the intellectual property across the worldwide enterprise.



Jo Stewart-Rattray / CSO at Silver Chain Group

Stewart-Rattray is the chief security officer at Silver Chain Group. She has over 25 years of experience in the IT field, some of which were spent as CIO in utilities and as group CIO in tourism. She also has significant experience in information security, including as a CISO in the healthcare sector. Stewart-Rattray specializes in consulting in risk and technology issues with an emphasis on governance and security in both the commercial and operational areas of businesses. She provides strategic advice to organizations across a number of industry sectors including banking and finance, utilities, manufacturing, tertiary education, retail, healthcare and government.



DATA BREACH

Third-Party Risk Concerns

TOM FIELD: After the year that we've had, what currently is your biggest concern about third-party risk?

JO STEWART-RATTRAY: The issue with third-party risk is that often we're just the collateral damage; it's not necessarily us that the attackers are after. It's perhaps our B2B with other organizations or in the government, and we're the collateral damage in the middle. But also with our third parties, whoever thought Microsoft was going to get hacked, or Kaseya, or SolarWinds? These are big names in the business. We have to be aware that it can happen to anybody and everybody. We have to ensure that we do proper risk assessments every time we bring a new vendor on, have the right conversations with vendors and have the right heads of agreement in place too that allow you the right to audit and the right to review.

RICHARD RUSHING: The numbers are against us. Most organizations have a multitude of third parties. We have everything from call centers to repair centers, service and support, all across the board and those are requiring deeper connectivity, deeper integrations and more functionality as things progress. It's like a tangled pile of spaghetti, and all those connections are entryways on the side of it. No matter what limitations you have and what controls you put into place, each one of those is a new vector for attackers, whether it's ransomware, APT nation-state groups,

cybercriminal organizations or the latest botnet. An attacker knows that if they can compromise one entity that has connections to multiple entities, they can leverage that to get to the next person. Why would they spend time attacking 15 or 100 different companies when they could attack one company and get 100 organizations under their control?


JAMIE WALSH: I'm concerned by how much of the data out there is sitting under the surface waiting to come back and bite you. A lot of things go undetected, and a lot of organizations are going to be surprised one day to find out that they spent weeks or months with an undetected breach that caught them off guard. A lot of organizations just don't realize how vulnerable they are.

STEWART-RATTRAY: It's nothing for an organization to be sitting there with an attack happening or having happened for nine to 18 months without realizing it. One day it just comes back to bite you; that's what we have to be aware of.

Breach Discovery and Contractual Issues

FIELD: How do you currently, ideally, discover a third-party breach?

RUSHING: Ideally, I would like for the third party to notify me according to the contractual obligations that they usually have. That rarely happens. In my



organization, we usually discover the breach long before the third parties are even aware of it and then when we point it out, they say, “No, it can’t be that.” There’s always a denial factor that we refer to as the “lawyer up” factor. The second you start communicating, the next thing you know there are lawyers on the call, and no questions will be answered because they’ll say, “This is under an active investigation, and we’ll get back to you with more details.”

One of the constant battles is that if you have the classic “castle and moat” or the “M&M strategy” for security, most of these organizations are already on the inside of your company and organization. If you haven’t architected the system correctly for your integrations, you’re going to have a world of hurt when you have to turn it off, do forensics and figure out what actually happened, and restore the service.

STEWART-RATTRAY: The bigger the organization that your third party is, the more you’ve got to check out the heads of agreement that you have with them because quite often you find that it’s incumbent upon you to say, “I think we’ve been breached because of you.” A lot of the companies will say that you cannot terminate the agreement because of a security breach on their side, but they can do it to you. So be aware of what is going into those heads of agreement and the bigger the company, the harder it is. We don’t tend to lawyer up quite so easily in Australia, but there’s still a deflection factor from organizations regardless of whether the lawyers are in the room

or not, and that’s a problem. Richard mentioned architecture: There’s architecture and there’s security architecture, and oftentimes the two are not the same. In fact, some enterprise architects do their damndest to undermine your security architecture. So you have to have that discussion, and oftentimes the CISO has to play the referee in between those two sides.

Organizations don’t particularly have a hard shell anymore. They have lots of B2B and lots of vendors coming in. You need to protect our data that’s within the network, and that’s hard because your perimeters have changed. The best you can do is monitor your vendors and make sure that you have good policies and procedures in place so we don’t give them free and unfettered access to the network. A vendor recently told me that in order for them to find out what the problem was, I had to let them run rampant in the network. I don’t think so. You have to guard against that and actively make sure that your people are working with the vendors to ensure that that doesn’t happen.

RUSHING: In contractual obligations, work with your legal team to get the language that you want. Find out what the notification time is. And put a penalty in the contract to say, “If we’re not notified of this, this could be terms for termination of the contract.” Use the word “incident.” If you say “breach,” they can say, “It’s not a breach; it’s an incident or an event.” Use the strongest legal words that your legal team feels comfortable using, and put some teeth in there.

STEWART-RATTRAY: You have to define all the terms: What does “significant” mean? What is a “significant breach” or a “significant incident”? What is an “incident”?

FIELD: Jamie, how do the organizations you deal with discover third-party breaches?

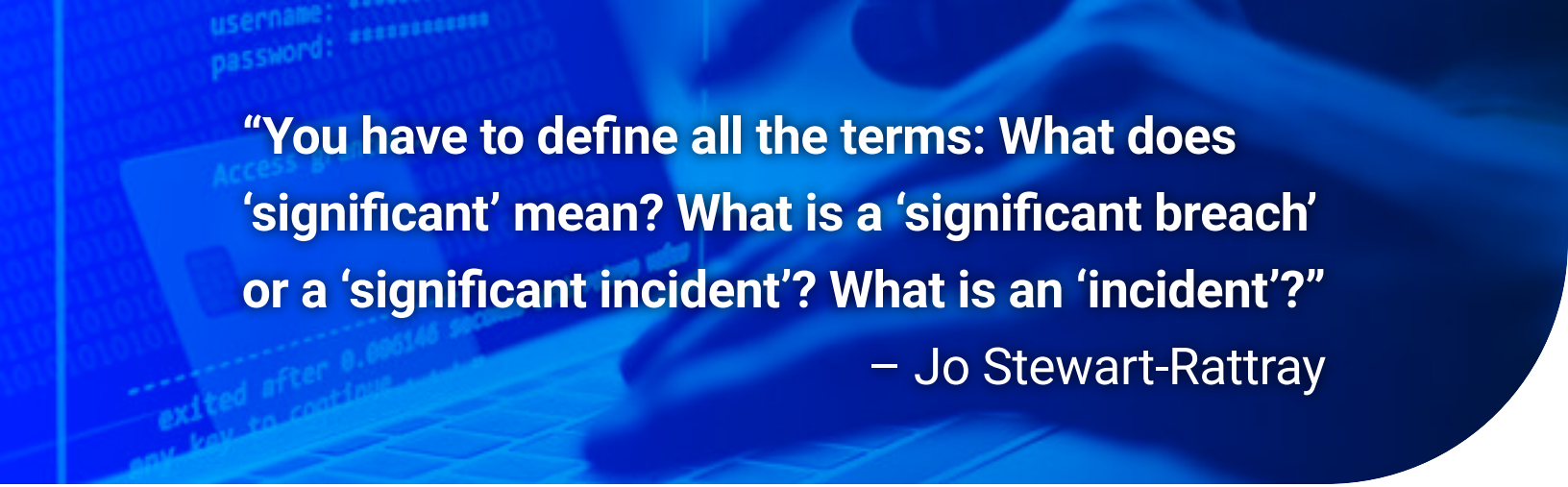
JAMIE WALSH: Ideally, the third parties bring the information to them as soon as possible. We have a lot of experience with both the buy side as well as the sell side of services, so we see people that are looking for solutions to help them stay resilient and then on the buy side, they’re looking at how to maintain third party relationships. A lot of organizations don’t look at contractual legalese on the sell side. They’re good at figuring out how to recover when something is going on, but they miss how to maintain continuity or communication strategy when something happens and knowing what their contractual obligation to meeting that is. You have to fix the breach as quickly as possible, but also recognize your contractual obligation

to alert the people that you are in business with as soon as possible. Ideally, it’s a partnership. You need to know who your partner is and treat it like a partnership because you’re going to end up in somewhat combative situations when things happen and there’s defensiveness. If you have a holistic view of what’s going on, and you’re proactively monitoring where your risk is happening or where something is about to blow up, and you have a plan in place for both the communication side and the recovery side, you can get through the entire crisis and get yourself back into a trust situation with your vendor or with your partner who’s buying services from you.

STEWART-RATTRAY: One of the issues around continuity is that oftentimes organizations completely forget their vendors or third parties, and they’ve got to be a part of it. You have to know what that third party’s continuity practice looks like because it can be left out of heads of agreement and if they have a disaster, you’re washed up as a result.

“An attacker knows that if they can compromise one entity that has connections to multiple entities, they can leverage that to get to the next person. Why would they spend time attacking 15 or 100 different companies when they could attack one company and get 100 organizations under their control?”

– Richard Rushing



“You have to define all the terms: What does ‘significant’ mean? What is a ‘significant breach’ or a ‘significant incident’? What is an ‘incident’?”

– Jo Stewart-Rattray

Gaps in Breach Detection

FIELD: Where do you see gaps in the technology that organizations often use now for detection?

WALSH: It’s about speed, and it’s about detection being tied to the right aspects of the business. We make sure that the context for what you’re monitoring from an IT perspective aligns with the business services that you are running to support whatever your business is. A key gap that we address quite often is making sure that they look at the business processes from a financial and legal perspective, understand the underlying interdependencies and what they touch, how often are they being monitored, and whether they have the right controls in place.

RUSHING: We can be sensitive about pushing mandates on vendors, and that’s a wrong approach. If they are connecting to your network, they should have to go through the same hurdles and same software detection scenarios that your employees do. Why should they be any different? Mandate it. We used to have development centers and call centers that were singly connected to the network, with 30 people working in a location. Now a lot of those people are working from home. We miss or do not calculate these pockets of the network where you have no visibility. If

you lack visibility in network traffic, logging and implementation, you’re flying blind. You need to have visibility across your enterprise at all different layers.

We confuse layers of security with defense in depth. The layers are just layers; they don’t serve a purpose. Defense in depth is designed so that if this misses it, this other safety net will catch it. We need to start defining things in defense in depth versus layers because with layers, you might have a gap that you completely miss and it’ll fall straight through the bottom. We’re all super busy with our staffs, and often the vendors and third parties are low on the totem pole.

STEWART-RATTRAY: Visibility is really important, and sometimes the lack of visibility involves things that you don’t expect. We live in an internet of things world; everything at some point is connected. These things are either on or passing over your network. They may or may not be air-gapped, so you have an issue of visibility. Can you see them? What kind of access do those vendors have to your network as a result? CISOs need to uncover that. We need to look for anomalous behavior across our networks, regardless of whether it’s coming from an IoT device or a more traditional device.

Breach Notification and Pausing Service

FIELD: Once a breach is discovered, what are your immediate responses regarding notification and pausing the engagement?

STEWART-RATTRAY: We have a very strong breach protocol. First, we determine that there has been a breach. If there has, we cut the third party off as soon as we possibly can. You have to have the playbooks in place to know what to do to shut them off and be able to continue business, and you have to play out the scenarios in your playbook.

RUSHING: You need to have a standard response process and run it. And with third parties, you need to have the right people in the room to make the decisions because of the complexity of all the network connections involved. Tell the vendor what they need to do to get back on the network. Give them the requirements, and make sure they understand them. Define the visibility that you need from them to be able to say, “We see that you remediated this. We can let you back on.” And you need to know how the vendor’s incident response plan is set up.

WALSH: If part of your recovery strategy is shutting off access when your third party is breached, you might want to have alternate

vendor strategies in place in case it’s a long-term disruption. If your breached third-party vendor is constantly telling you, “I will get back to you,” that’s a red flag that they don’t have their incident response plan together. And that will make it hard for them to gain your trust back.

Whose Remediation Is It?

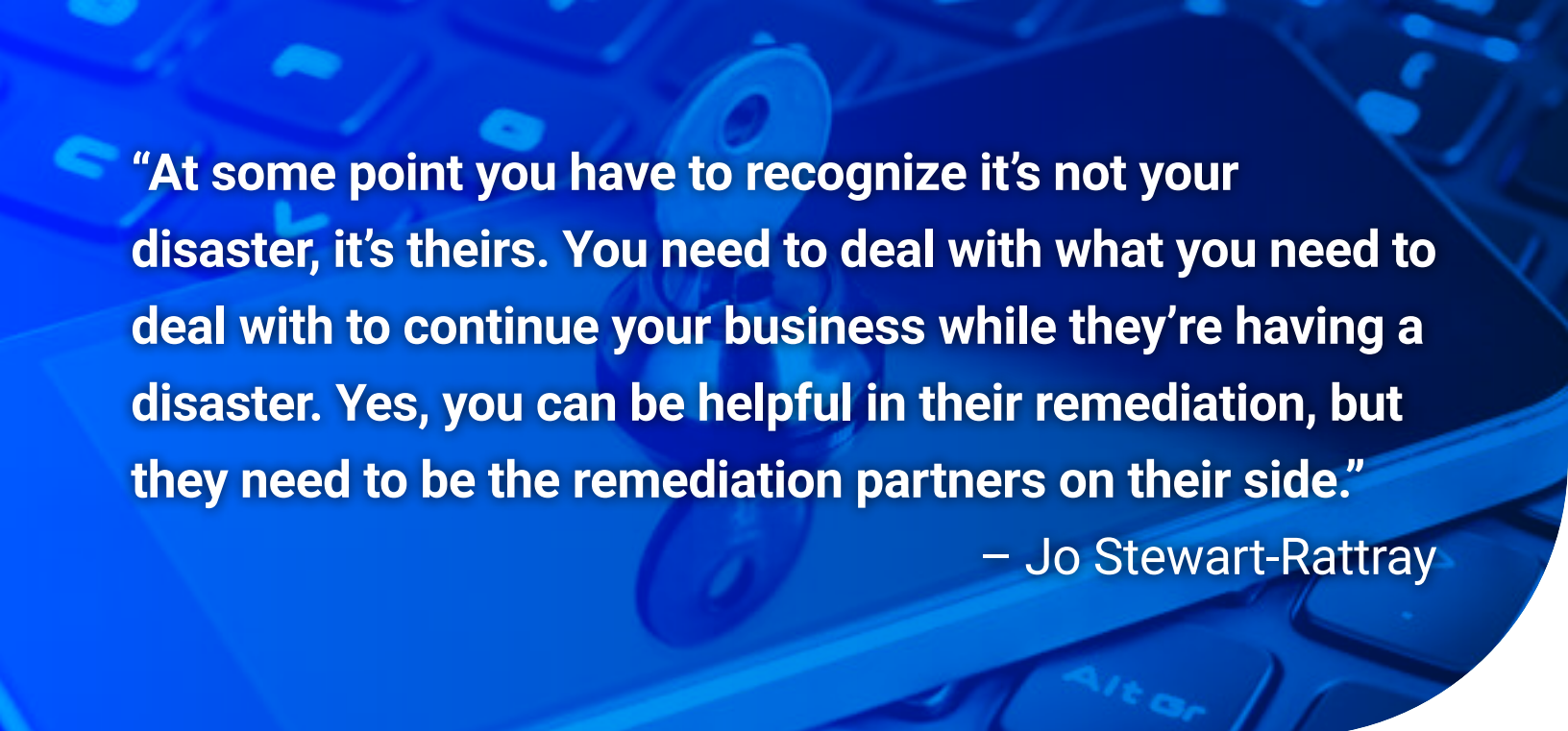
FIELD: To what degree are you engaged in the partner’s remediation process?

RUSHING: You’re probably engaged as much as the vendor needs you or wants you. In some situations, you’re almost running their recovery process or you’re asking questions and they are stumbling around. You shouldn’t be part of it; they should be able to recover on their own, but in a lot of cases you’re left with the recovery or partial recovery. And it’s hard to continue to do business with them during that. Can you use email to send them files? Are they blocking your email address? You can go to paper, but how does the paper get transacted at that point in time?

This is the stuff that no one has sat down and thought about, in a lot of cases. They’ve thought about the protection and the detection side of it, but not the recovery side. Do you take all your

“If your breached third-party vendor is constantly telling you, ‘I will get back to you,’ that’s a red flag that they don’t have their incident response plan together. And that will make it hard for them to gain your trust back.”

– Jamie Walsh



“At some point you have to recognize it’s not your disaster, it’s theirs. You need to deal with what you need to deal with to continue your business while they’re having a disaster. Yes, you can be helpful in their remediation, but they need to be the remediation partners on their side.”

– Jo Stewart-Rattray

equipment and throw it in the dumpster? How do you segment it? How do you go back and build a new network? Because if a site or an organization was compromised, how do you trust anything that was there? And that becomes, “We’re building a whole new network. We plugged our PCs on this network and then we plugged them onto the new network.” And that defeats the whole purpose of building a whole new network.

Don’t cross the streams. It’s air-gapped; do not cross this. A constant problem is that they are trying to do service restoration from IT instead of recovery from the incident that happened. It’s a recovery process; it’s not system restoration yet. Don’t even try to push the envelope; get everything situated first and then move on. Ask for updates on the process. If you don’t get them, that means the process is not going according to plan: They said two days, but it’s already been a week and there’s still no update. Maybe they overestimated. Maybe they’re having trouble. If so, you need to tell your business leaders that it’s going to take a lot longer than you expected.

STEWART-RATTRAY: At some point you have to recognize it’s not your disaster, it’s theirs. You need to deal with what you need to deal with to continue your business while they’re having a disaster. Yes, you can be helpful in their remediation, but they need to be the remediation partners on their side. And your executive leadership team may decide to cut ties with that organization and determine if, contractually, you can terminate the agreement. You need to consider who the vendor is and what they are doing for you. You need to have the channels of communication open and talk to your CEO to make sure they are continually updated, so they’re not reading stuff in the press about what’s going on with the vendor.

WALSH: Communication is definitely crucial. If the vendor is hesitant about providing documentation and you are not hearing updates, that could mean you are not going to restore confidence with this vendor and you need to part ways or branch off and start your own recovery strategy with another vendor that might be able to provide this service in a few weeks or so, pretty quickly. It’s key to

build that into your plan. Your relationship with the vendor is a partnership, so you want to give them an opportunity to go through this but you also want to get a feel for what they do on a regular basis to harden and practice their recovery strategies and what types of communication can you expect. That way, you can have a great partnership and not just a vendor that's providing a service and it's black hole when things get rough.

Dealing With Vendors Post-Breach

FIELD: What does it take to get a partner back on board?

WALSH: You need evidence from an independent third party to validate that forensically the partner is clean, they're back and they're ready to go. You want to take their word for it, but before you turn that switch back on and give them access back into your network, there's usually some paperwork that needs to be filled out from somebody that you trust.

STEWART-RATTRAY: It's important to make sure that you're confident that they're clean and that they've done the right thing. Also, do you want them back on board? That's the big discussion.

Oftentimes, these things happen with vendors that you don't have a great trust relationship with. If you don't want them back on board, you need to decide what to do. If it's appropriate to cut the ties, cut the ties.

RUSHING: Be sure to take your time. Give them access to things that they may need, but do your service restoration in phases. In phase one, let the vendor talk to this system and this system only. And watch them. You can have a three-strike rule. After the third strike, you're done with them. Document things and communicate. For example, say, "If this works well and we're good for the next 48 hours, we'll turn the next server on, and we'll turn the next one on after that." Do it at your speed; don't just jump into the deep end of the pool.

Internal Pushback

FIELD: What kind of internal pushback can you expect when you want to pause a supply chain because of a breach or an incident?

RUSHING: That third party is providing services for some part of your organization, and you will get pushback. Understand who owns that relationship, and tell them and integrate them first. Most likely, if

"You need evidence from an independent third party to validate that forensically the partner is clean, they're back and they're ready to go. There's usually some paperwork that needs to be filled out from somebody that you trust."

– Jamie Walsh

you say, “This vendor is infected with ransomware or has malware, and it tried to infect our organization and shut down something,” they’ll let you make the call. If they don’t, you’re going to be in between two VPs and a rock and a hard place.

STEWART-RATTRAY: You’ve got to have continuing communication. The other kind of pushback you can get is when executives don’t understand, and they say, “Just cut them off. Get rid of them. Get somebody else.” Then you need to make those leaders understand what this vendor does for you and what it means to you, the partnership that you have in place and the contractual obligations. CISOs need to be patient and have those discussion internally.

WALSH: Testing and regular exercising of various scenarios is important, and that should include: What do we do if this particular vendor falls off the face of the earth or we have a disruption where we have to cut them off? Have that discussion with the business leaders that are in charge of the revenue-generating process and understand the impact if this area of the business is disrupted for

three days or 30 days. Have those conversations on a regular basis; even once a year is vital, especially with turnover internally, turnover of vendors, and ever-changing business scenarios.

Maintaining Business Continuity

FIELD: How do you maintain business continuity and resilience while all this is happening?

STEWART-RATTRAY: It has to be enshrined in your day-to-day practices. You have to be ready for an event or an incident and have playbooks so that when it happens, you can do something about it. You have to make sure you are a very well-organized, well-oiled machine that can move into the resilience phase. Go through the practice. If your plans and materials are online, make sure you can access them. Put them in multiple places. Keep your resilience processes modern, up to date and flexible.

RUSHING: While the issue is going on, business leaders will ask, “How many other vendors is this

“Consider the lessons learned from the incident and recover and record that information. If you don’t figure out what worked, what didn’t work, and what you would change, you’re going to relive this on a regular basis. And if it was a nightmare, it’s going to be another nightmare because you didn’t change anything.”

– Richard Rushing

critical for? And you need to tell them, “Let us finish this before we start the next one.” You can’t stretch people in an infinite number of ways. And you have to consider the lessons learned from the incident and recover and record that information. If you don’t figure out what worked, what didn’t work, and what you would change, you’re going to relive this on a regular basis. And if it was a nightmare, it’s going to be another nightmare because you didn’t change anything.

WALSH: Look at risk monitoring for IT and operational risk and third-party risk. Figure out strategies and risk tolerances. Codify appropriate actions so that when things go wrong, you have a quick plan to execute on a moment’s notice. Do regular testing. Rehearse your plan, Learn from every mistake, and revise your action plan based on those findings. Then execute and implement the plan efficiently when things go wrong. All that plays a part in business resiliency.

Partner Validation

FIELD: How must your partner validate its security remediation?

WALSH: Documentation is key. There are not a lot of ways that you can do on-site inspection and auditing during this. You’re trying to get things done quickly, so it’s good to have trusted third parties in the area where your critical vendors work and operate.

STEWART-RATTRAY: The validation piece is an independent third-party review. It has to be done quickly, and it has to give you what you need so you can be confident that everything is all right. Richard mentioned a three-strike rule, but you only

get two with me. The first time, it’s an accident; the second time, it’s goodbye.

RUSHING: You need some level of evidence: How many hosts were infected with this? What were they infected with? What happened and how was it done? Did any of my data go out your door? You can directly ask the third party those things, and they need to be able to answer them before you consider bringing them back online. Make sure they know that it is a consideration and not a given fact that you’re going to give their access back. Ask very specific questions: What malware was there? Were there any indicators of compromise that you could use on your side? Ask them what they did to remediate. You need to know what they did to clean up their environment. They should be able to document that very well. Also, think about what you would be willing to provide to a third party to tell them that you’re clean.

The SAI Approach

FIELD: How is SAI helping its customers address these issues we’ve talked about here?

WALSH: We are launching business resilience as a package. We have a number of different solutions for business continuity, third-party risk, IT risk, and enterprise and operational risk. We also have solutions that deal with regulatory compliance risk. We’re bringing those together so you can proactively monitor all of the different risk terrains that you have within your organization, develop plans and strategies that you can exercise and test, and give your third parties the ability to communicate and resolve issues collaboratively with you – both when things are going wrong and when you’re establishing trust in the first place.



Our mission is a connected approach to risk management

SAI360 is the leading provider of Risk, Learning, EHS, and Sustainability software. Our unified approach to risk management is what sets us apart, helping organizations across the globe manage risk, create trust, and achieve business resilience for over 25 years.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

 **BANK INFO SECURITY®**  Just for Credit Unions **CU INFO SECURITY®**  **GOV INFO SECURITY®**  **HEALTHCARE INFO SECURITY®**

 **infoRisk**
TODAY®

 **CAREERS INFO SECURITY®**

Data Breach.
Prevention. Response. Notification. TODAY

CyberEd.io


ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io