Building a Vendor (IT) Risk Management Program

Version 1.3
Released: April 28, 2016

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author’s Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper and John Moltz for editing and content support.

This report is licensed by BitSight.

www.bitsighttech.com

BitSight Technologies is transforming how companies manage information security risk with objective, evidence-based security ratings. The company's Security Rating Platform continuously analyzes vast amounts of external data on security behaviors in order to help organizations manage third-party risk, benchmark performance, and assess and negotiate cyber insurance premiums. Based in Cambridge, MA, BitSight is backed by the National Science Foundation, Globespan Capital Partners, Menlo Ventures, Flybridge Capital Partners, Comcast Ventures, Commonwealth Capital Ventures, Liberty Global Ventures, Shaun McConnon, and Singtel Innov8. For more information, please visit www.bitsighttech.com, read our blog or follow @BitSight on Twitter.

Copyright

Building a Vendor (IT) Risk Management Program

Table of Contents

Understanding Vendor IT Risk

Outsourcing is nothing new. Industries have been embracing service providers for functions they either couldn't or didn't want to perform for years. This necessitated integrating business systems and providing these third-party vendors with access to corporate networks and computer systems. The risk was generally deemed manageable and rationalized by the business need for those integrated processes. Until it wasn't.

The post-mortem on a few recent high-profile data breaches indicated the adversaries first entered the victim's network not through their own systems, but instead through a trusted connection with a third-party vendor. Basically the attacker targeted and then owned a small service provider, and used that connection to gain a foothold within the real target's environment. The path of least resistance into your environment may no longer be through your front door. It might be through a back door (or window) you left open for a trading partner.

The path of least resistance into your environment may no longer be through your front door. It might be through a back door (or window) you left open for a trading partner.

Business will continue to take place, and you will need to provide access to third parties. Saying 'no' is not an option. Yet you can no longer just ignore the risks vendors present. These vendor connections dramatically expand your attack surface, which now includes the environments of all the third parties with access to your systems. Ugh.

This could be thousands of different vendors. No, we aren't forgetting that most of you don't have the skills or resources to stay on top of your own technology infrastructure — not to mention critical data moving to cloud resources. Now you also need to worry about all those other organizations you can neither control nor effectively influence. Horrifying.

This is when you expect Tom Cruise to show up, because this sounds like the plot to the latest *Mission: Impossible* sequel. Unfortunately this is your lot in life. Yet there is hope, because services are emerging that evaluate (and rate) the IT risk posed by trading partners and vendors, without needing access to their networks.

In this *Building a Vendor (IT) Risk Management Program* paper we will go into why you can no longer ignore vendor risk, and how these services can actually pinpoint malicious activity on your vendors' networks. But just having that information is (no surprise) not enough. To efficiently and effectively manage vendor risk you need a systematic program to evaluate dangers to your organization and objectively mitigate them.

Regulation

You know an issue has been obvious for a while when regulators establish guidance to address the problem. Back in 2013 the regulators overseeing financial institutions in the US seemed to get religion about the need to assess and monitor vendor risk, and IT risk was a subset of the guidance they produced. Of course, as with most regulation, enforcement has been spotty and didn't really offer a prescriptive description of what a vendor risk management program consists of. It's not like the 12 (relatively) detailed requirements you get with the PCI-DSS.

In general, the guidance covers some pretty straightforward concepts. First you should actually write down your risk management program, and then perform proper due diligence in selecting third parties to work with. I guess you figure out what "proper" means when the assessor shows up and lets you know that your approach was improper. Next you need to monitor vendors on an ongoing basis and have contingency plans in case one screws up and you need to get out of the deal. Finally you need program oversight and documentation, so you can know your program is operational and effective. Not brain surgery, but also not very specific.

The most detail in any guidance we found comes from the OCC (Office of the Comptroller of the Currency), which recommends an assessment of each vendor's security program in its Risk Management Guidance.

> Information Security
>
> Assess the third party's information security program. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology is necessary to support service delivery, assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests. Evaluate the third party's ability to implement effective and sustainable corrective actions to address deficiencies discovered during testing.
>
> - OCC Risk Management Guidance

No problem, right? Especially for those of you with hundreds (or even thousands) of vendors within the scope of assessment. You can just add it to the list and bang through it. Yup.

We'll add our standard disclaimer here, that *compliance doesn't make you secure.* It cannot make your vendors secure either. But it does give you a reason to allocate some funding to assessing your vendors and making sure you understand how they affect your attack surface and exploitability.

The Need for a Third-Party Risk Program

Our long-time readers won't be surprised that we prescribe a program to address a security need. Managing vendor IT risk is no different. In order to achieve consistent results, and be able to answer your audit committee about vendor risk, you need a systematic approach to plan the work and then work the plan.

Structuring the Program

Modern integrated business processes have dramatically expanded the attack surface of pretty much every organization. You can no longer ignore the risk presented by vendors or other business partners, even without regulatory bodies pushing for formal risk management of vendors and third parties. As security program fanatics we figure it is time to start documenting such a program.

Defining a Program

First let's define what we mean by a *security program*. The first thing a program needs is to be systematic, which means you don't do things willy-nilly. You plan the work and then work the plan. The processes involved in the program need to be predictable and repeatable. Well, as predictable as anything in security can be. Here are some other hallmarks of a program:

- **Executive Sponsorship:** Our research shows a security program has a much higher chance of success if there is an executive (not the CISO) who feels accountable for its success. Inevitably security involves changing processes, and maybe not doing things business or other IT groups want because of excessive risk. Without empowerment to make those decisions and have them stick, most security programs die on the vine. A senior sponsor can break down walls and push through tough decisions, making the difference between success and failure.
- **Funding:** Regardless of which aspect of security you are trying to systematize, it costs money. This contributes to another key reason programs fail: lack of resources. We also see a lot of organizations kickstart new programs by just throwing new responsibilities at existing employees, with no additional compensation or backfill for their otherwise overflowing plates. That's not sustainable, so a key aspect of program establishment is allocating money to the initiative.
- **Governance:** Who is responsible for operation of the program? Who makes decisions when it needs to evolve? What is the escalation path when someone doesn't play nice or meet agreed-upon responsibilities? Without proper definition of responsibilities and sufficient documentation so revisionist history isn't a factor, the program won't be sustainable. These roles need to be defined when the program is being formally established, because it's much easier to make these decisions and get everyone on board before it goes live. If it does not go well people will run for cover, and if the program is a success everyone will want credit.

- **Operations:** This will vary greatly between different kinds of programs, but you need to define how you will achieve your program goals. This is the 'how' of the program, and don't forget about an ongoing feedback and improvement loop so the program continues to evolve.

- **Success criteria:** In security this can be a bit slippery, but it's hard to claim success without everyone agreeing what success means. Spend some time during program establishment to focus on applicable metrics, and be clear about what success looks like. Of course you can change your definition once you get going and learn what is realistic and necessary, but if you fail to establish it up front, you will have a hard time showing value.

- **Integration points:** No program stands alone, so there will be integration points with other groups or functions within the organization. Maybe you need data feeds from the security monitoring group, or entitlements from the identity group. Maybe your program defines actions required from other groups. If the ultimate success of your program depends on other teams or functions within the organization (and it does, because security doesn't stand alone), then making sure everyone is crystal clear about integration points and responsibilities from the beginning is critical.

The V(IT)RM Program

To tailor the generic structure above to vendor IT risk management you need to go through the list, make some decisions, and get everyone on board. Sounds easy, right? Not so much, but doing this kind of work now will save you from buying Tums by the case as your program goes operational.

Our research shows a security program has a much higher chance of success if there is an executive (not the CISO) who feels accountable for its success.

We cannot tell you exactly what governance and accountability needs to look like for your program because that is heavily dependent on your culture and organization. Just make sure someone is accountable and operational responsibilities are defined. In some cases this kind of program resides within a business unit managing vendor relationships, other times it's within a central risk management group, or it could be somewhere else. You need to figure out what will work in your environment for your organization.

One thing to pay close attention to, particularly for risk management, is contracts. You enter business agreements with vendors every day, so make sure the contract language reflects your vendor risk management program objectives. If you want to scan vendor environments for vulnerabilities, that needs to be in your contracts. If you want them to do an extensive self-survey or provide a data center tour, that needs to be there. If your contracts don't include this kind of language, look at adding an addendum or forcing a contract overhaul at some point. That's a decision for the business owners that manage your vendors.

- **Defining Vendor Risk:** The first key requirement of a vendor risk management program is actually defining categories in which to group your vendors. These categories define the basis for your operation of the entire program. You will need to categorize both vendors and the risks they present so you know what actions to take, depending on the importance of the vendor and the type of risk.
- **Operations:** How will you evaluate the risk posed by each vendor? Where will you get the information and how will you analyze it? Do you reward organizations for top-tier security? What happens when a vendor is a flaming pile of IT security failure? Will you just talk to them and inform them of the issues? Will you lock them out of your systems? It will be controversial if you take a vendor off-line, so you need to have had all these discussions with all your stakeholders before any action takes place. This is why we constantly beat the drum for documentation and consensus when establishing a program.
- **Success Criteria/Metrics:** There is of course only one metric that is truly important, and that's whether a breach resulted from a vendor connection. OK, maybe that's a bit overstated, but that is what the Board of Directors will focus on. Success likely means no breaches due to vendor exposure. Operationally you can set metrics around the number of vendors assessed (100% may not be practical if you have thousands of vendors), or perhaps how many vendors are in each category, and what the direction of the trend is. There is only so much you can do to impact the security posture of your vendors, but you can certainly take action to protect yourself if a vendor is deemed to pose an unacceptable risk.
- **Tuning:** In a V(IT)RM program, the categories of importance and risk are the most critical information. So when tuning the program over time, you want to know how many of your vendors were breached and whether any of those breaches resulted in loss to you. If there was a breach, did you identify the risk ahead of time — basically having a good idea that vendor would have an issue — or was this a surprise? The objectives of tuning are to eliminate surprises and wasted effort.

Of course many aspects of the program, if not all, change over time as technology improves and requirements evolve. That is to be expected, and part of the program has to be a specific set of activities focused around gathering feedback and tuning the program as described above. We also believe strongly that programs need to be documented (yes, written down), so if (or should we say when) something goes wrong you have documentation that someone else understood the potential issues and accepted the risk. Even if you write it in pencil, write it and make sure all of the stakeholders understand what they agreed to.

Evaluating Vendor Risk

Now with a program structure to manage the risk, it begs the question of how do you actually evaluate the risks of a vendor? What should you be worried about, and how can you gather enough information to make an objective judgement of the risk posed by every vendor?

Risk in the Eye of the Beholder

The first aspect of evaluating vendor risk is actually defining what that risk means to your organization. Yes, that seems self-evident, but you'd be surprised how many organizations don't document or get agreement on what presents vendor risk, and then wonder why their risk management programs never get anywhere. Sigh.

All the same, as mentioned above, vendor (IT) risk is a component of a larger enterprise risk management program. So the first step is to establish the risks of working with vendors. Those risks can be broken up into a variety of buckets, including:

- **Financial:** This is about the viability of your vendors. Obviously this isn't something you can control from an IT perspective, but if a key vendor goes belly up, that's a bad day for your organization. So this needs to be factored in at the enterprise level, as well as considered from an IT perspective — especially as cloud services and SaaS proliferate. If your Database as a Service vendor (or any key service provider) goes away, for whatever reason, that presents risk to your organization.
- **Operational:** You contract with vendors to do something for your organization. What is the risk if they cannot meet those commitments? Or if they violate service level agreements? Again it is enterprise-level risk of the organization, but it also peeks down into the IT world. Do you pack up shop and go somewhere else if your vendor's service is down for a day? Are your applications and/or infrastructure portable enough to even do that?
- **Security:** As security professionals this is our happy place. Or unhappy place, depending on how you feel about the challenges of securing much of anything nowadays. This gets to the risk of a vendor being hacked and losing your key data, impacting availability of your services, and/or allowing an adversary to jump across into your networks and systems via their network.

Within those buckets, there are probably a hundred different aspects that present risk to your organization. After defining those buckets of risk, you need to dig into the next level and figure out not just what presents risk, but also how to evaluate and quantify that risk. What data do you need to evaluate the financial viability of a vendor? How can you assess the operational competency of vendors? And finally, what can you do to stay on top of the security risk presented by vendors? We aren't going to tackle financial or operational risk categories, but we'll dig into the IT security aspects below.

Ask them

The first hoop most vendors have to jump through is self-assessment. As a vendor to a number of larger organizations, we are very familiar with the huge Excel spreadsheet or web app built to assess our security controls. Regardless of the fact that our small shop has more sophisticated controls than a lot of really big companies, we still need to go through each cell of the spreadsheet to detail our defenses. Most of the questions revolve around organizational policies, controls, response, and remediation capabilities.

The path of least resistance for this self-assessment is usually a list of standard controls. Many organizations start with ISO 27002, COBIT, and/or PCI-DSS. Relevance is key here. For example, if a vendor is only providing your organization with nuts and bolts, their email doesn't present a very significant risk to your organization. So you likely want a separate self-assessment tool for each risk tier, as we'll discuss below.

An aspect of the self-assessment that you need to factor in is honesty. It is not hard to lie on a spreadsheet or web application. And some vendors do exactly that. But you don't have the resources to check everything, so there is a measure of trust involved. Although you should statistically verify some of the vendors and make a big deal if an organization is caught bending the truth. That sends a message to the other vendors. Just remember that it is resource-intensive to evaluate every answer, so focus on what's important based on how your organization defines vendor risk.

> You'd be surprised how many organizations don't document or get agreement on what presents vendor risk, and then wonder why their risk management programs never get anywhere. Sigh.

External information

Just a few years ago, if you wanted to assess the security risk of a vendor, you needed to either have an on-site visit or pay for a penetration test to really see what an attacker could do to the vendor. That required a lot of negotiation and coordination with the vendor, which meant it could only be used for your most critical vendors, and not often even for them. And they are likely to tell you to go pound sand, pointing to the extensive self-assessment you forced them to fill out.

But now, with the introduction of security rating services, and techniques you can implement yourself, you can get a sense of what kind of security mess your vendors actually are.

Here are a few types of relevant data sources:

- **Botnets:** Botnets are public by definition because they use compromised devices on public networks to communicate with each other. So if a botnet is penetrated, you can see who is connecting to it at the time and get a pretty good idea of which organizations have compromised devices. That's exactly how a number of services tell you that certain networks are compromised without ever looking at the networks in question.
- **Spam:** If you have a network that is blasting out a bunch of spam, that indicates an issue. It's straightforward to set up a number of dummy email accounts to gather spam and see which networks are used to blast millions of messages a day. If a vendor owns one of those networks, that's a disheartening indication of their security prowess.
- **Stolen credentials:** There are a bunch of forums where stolen credentials are traded and if a specific vendor shows up with tons of their accounts and passwords for sale, that means their security probably leaves a bit to be desired.
- **Malware distribution/infected hosts:** Another indication of security failure is Internet-facing devices which are compromised and then used to either host phishing sites or distribute malware, or both. If a vendor's Internet site is infected and distributing malware, they likely have no idea what they are doing.
- **Public Breaches:** We'll discuss this later, but if your vendor is a public company or deals with consumers, they have to disclose breaches to their customers. Although you've likely gotten kind of numb to yet another breach notification, if it mentions a key vendor, that's a concern. We'll discuss what to do when a vendor is breached later in this paper.
- **Security Best Practices:** There are also other tells that a vendor knows a bit about security. Do they encrypt all traffic to/from their public sites? Do they authenticate their email with technologies like SPF or DKIM? Do they use secure DNS requests? To be clear, these aren't conclusive indicators, but they can certainly give you a clue to how serious a vendor is about security.

> An aspect of the self-assessment that you need to factor in is honesty. It is not hard to lie on a spreadsheet or web application. And some vendors do exactly that.

So how do you gather all of this information? You can certainly do it yourself. Set up a bunch of honeypots and dedicate some internal resources to mining through the data. If you have tens of thousands of vendors and are heavily regulated, you might do exactly this. Otherwise you'll likely rely on an external information provider to perform this analysis for you.

We covered some aspects of these services in our Ecosystem Risk Management Paper, and we'll quickly summarize here. You need to figure out if you are looking for this vendor to provide a score and ranking of your other vendors, or whether you want the raw data on which vendors have issues (whether with botnets, malware distribution, etc.) to perform your own analysis and draw your own conclusions.

Risk Tiers

To make this kind of program feasible, without requiring another 25 bodies, let's discuss risk tiering. Larger organizations may have thousands of vendors. It's hard to consistently perform deep risk analysis of every vendor you do business with. But you also cannot afford only a cursory look at a few key vendors which present significant risk to *your* organization. You address this limitation by tiering different vendors into separate risk tiers.

We're simple folks, so we find any more than 3 or 4 tiers unwieldy. *One of your first actions, after defining your vendor IT security risk, is to nail down and build consensus on how to tier vendors by risk.* Then your analyses and assessments will be based on the risk tier, and not some arbitrary decision on how deeply to look at each vendor. You could use tiers such as: critical, important, and basic. (You could call them "unimportant" vendors but that might damage their self-esteem.) The names don't matter — you just need a set of tiers to group them into.

> It's hard to consistently perform deep risk analysis of every vendor you do business with. But you also cannot afford only a cursory look at a few key vendors which present significant risk to your organization.

Critical vendors will get the full boat: a self-assessment, a means to externally evaluate their security posture, and possibly a site visit. You'll scrutinize their self-assessments and have alerts triggered when something changes with them. We'll go into what options you have to deal with vendor risk later in the paper, but for now suffice it to say you'll be all over your critical vendors, to make sure they are secure and have a plan to address any deficiencies.

Important vendors may warrant a cursory look at the self-assessment and the external evaluation. The security bar might need to be lower for these folks, because they present less risk to your organization. Basic vendors send in their self-assessment, and maybe you perform a simple vulnerability scan on their external web properties, just to check some box on an auditor's checklist. That's about all you'll have time for with these folks.

Could you have more risk tiers? Absolutely. But the amount of work increases exponentially with each additional tier. That's why we favor only using a handful, knowing that from a risk management standpoint the best bang for your buck will be from focusing on your critical vendors.

Tracking over Time

Obviously security is highly dynamic, so what is secure today might not be tomorrow. Likewise, what was a mess a month ago may not be so bad right now. Yet most vendor risk assessments provide a single point-in-time view, representing what things looked like at that moment. Such an assessment has limited value, because every organization can have the proverbial bad day and inevitably some data sources provide false positives.

You want to evaluate each partner over time and track their progress. Have they shown fewer infected hosts over time? How long does it take them to remediate devices participating in botnets? Has a vendor that traditionally did security well suddenly started blasting spam and joining a bunch of botnets? Part of defining your vendor (IT) risk management program is figuring out which of the quantitative risk metrics most closely represent real risk to your organization and need to be tracked and managed over time.

Ongoing Monitoring and Communication

After you figure out what risk means to your organization and determine the best way to quantify and rank your vendors relative to that concept of risk, you'll do an initial risk assessment and figure out which vendors are a cesspool of security fail and need immediate attention. After going through that initial wave, you'll need to revisit your risk assessment at some point since security and the vendor's environment is dynamic and constantly changing.

Ongoing monitoring

When you think about keeping tabs on your vendors, you'll need to decide how often you want to update your assessment of their security posture. In a perfect world, you'd like to have a continuous view of each vendor's environment to be able to understand your risk at all times. Of course, there is a cost to continuous monitoring. So part of defining the V(IT)RM program is to figure out the frequency of the assessment.

We believe that not all vendors should be treated alike. The vendors you rate in critical risk tier (as described above) should be assessed as often as possible. Preferably you'll have a means (most likely third party services) of looking at their Internet footprint continuously and alerting you when something adversely changes. Although we need to caveat that statement with the reality of real-time alerts. If you are not staffed to deal with real-time alerts, then getting the alerts faster doesn't really help you. In other words, if it takes you 3 days to work through the alert queue, getting an alert within an hour isn't going to reduce your risk too much.

Vendors in the less risky tiers can be assessed less frequently. Maybe an annual self-assessment and a quarterly scan is enough for those partners. Again, this will be determined by your ability to deal with issues and verify answers. If you aren't going to look at the results, forcing the vendor to update their self-assessment quarterly is just mean, so be honest with yourself when determining the proper frequency for assessments.

With the frequency of assessment determined by risk tier, then what? You'll get a certain number of your vendors that have adverse changes to their security posture. The next aspect of the V(IT)RM program is to figure out how to deal with these vendor issues.

Taking Action

You've gotten an alert that there is an issue with the vendor and you'll need to take action. But what actions can you take considering the risk of the issue and the contractual agreement already in place? We can't really minimize the importance of defining acceptable actions contractually as part of the on-boarding process. That means a critical aspect of the setup and initiation of the program is going to be ensuring the contractual vehicles in place with the vendors support your desired actions when an issue arises.

So what can you do? This list is pretty consistent with most other security processes:

- **Alert:** At a minimum, you'll want to have a line of communication open with the vendor to tell them you've found an issue. This is no different from an escalation during an incident response. You'll need to assemble the information you've found and package that up for the vendor to give them as much information as is practical. Although you'll need to balance how much time you're willing to spend helping the vendor with everything else on your todo list.
- **Quarantine:** As an interim measure until you can figure out what happened and what the best course of action is, you could quarantine the vendor. That could mean a lot of things. Maybe it's about segmenting their traffic from the rest of your network. Or you may need to scrutinize each transaction with that vendor. Or analyzing all egress traffic to the vendor ensuring there is no leaking intellectual property. The point here is that you'll need time to figure out the best course of action, and putting the vendor in the proverbial penalty box can buy you that time. This is also contingent on being able to put a boundary around a specific vendor or service provider, which may not be possible given what service(s) they provide.
- **Cut off:** There is also the kill switch, which removes vendor access from your systems and likely ends the business relationship. Of course, this is a pretty draconian action, but sometimes a vendor presents such risk and doesn't make the changes you require that you may not have a choice. As mentioned above, you'll need to make sure the contractual relationship with the vendor allows this action. Unless you look forward to extended litigation with the vendor.

> The vendors you rate in critical risk tier (as described above) should be assessed as often as possible. Preferably you'll have a means (most likely third party services) of looking at their Internet footprint continuously and alerting you when something adversely changes.

The latter two options will necessarily impact the flow of business between your organization and the vendor, so you'll need to have a process to internally determine if/when you quarantine and/or cut off a specific vendor from your systems. This escalation and action plan needs to be defined ahead of time. The rules of engagement and the criteria to end a business relationship due to IT risk need to be established ahead of time. Defined escalations ensure the internal stakeholders are in the loop as you consider flipping the kill switch.

A good rule of thumb is that you don't want to surprise anyone when a vendor goes into quarantine or is cut off from your systems. If the business decision is made to keep the vendor in your systems (a decision that would be made well above your pay grade), then at least you have the documentation that the risk was accepted by the business owner.

Communicating Issues

Once the action plan is defined, documented and agreed upon, you'll want to build a communication plan. That involves defining when you'll notify the vendor and when you'll communicate the issue internally. As part of the vendor on-boarding process, you need to define the points of contact with the vendor. Do they have a security team that you should interface with? Is it their business operational group? Either way, you need to know this before you run into an issue.

You'll also want to make sure to have an internal discussion about the degree you'll support the vendor as they work through any issues that you find. If the vendor has an immature security team/program you can easily end up doing a lot of work for them. And it's not like you have a bunch of time to do someone else's work, right?

To be clear, business owners may not be exactly sympathetic to your plight when their key vendor needs to be cut off. That's why organizational buy-in on the criteria for quarantining or cutting a vendor off is critical. The last thing you as the security professional want is to be in a firefight with a business leader over a key vendor. Establish your criteria and manage to that criteria. If you are overruled and the decision is to make an exception to the criteria, you can't do much about that. But at least you are on record that the decision goes against the policies established within the vendor risk management program.

To be clear, business owners may not be exactly sympathetic to your plight when their key vendor needs to be cut off. That's why organizational buy-in on the criteria for quarantining or cutting a vendor off is critical.

Breach Exposure

If you have enough vendors, you'll run into the situation where your vendor suffers a public breach. You'll need to specifically factor that into your program because you may have a responsibility to disclose the 3rd party breach to your customers as well. First things first, the vendor breach shouldn't be a surprise to you. A vendor should proactively call their customers when they are breached and a customer is at risk. Yet this is the real world, so assuming they'll act correctly is probably a bad assumption. So what then?

This gets back to the incident response playbook in place for your organization. You have that documented, right? As we described in our incident response fundamentals research, you need to size up the issue, build a team, assess the damage and then move to contain it. Of course, this is a bit different because there will be a lot that you don't know since it wasn't your systems that were breached. And depending on the sophistication of the vendor, they may not know either.

So (as always) internal communication and keeping senior management apprised of the situation is critical. You'll need to stay in close contact with the vendor and constantly assess your level of exposure and if/when you'd need to disclose to your board, audit committee or possibly customers.

Also, as described in the I/R fundamentals research, make sure to work through a post-mortem with the vendor to make sure they have learned. If you aren't satisfied it won't happen again, then perhaps you need to escalate to the business to reevaluate the business relationship given the additional risk involved in doing business with them. Also use this as an opportunity to refine your own process for the next time a vendor is popped.

Summary

Whether resulting from high profile breaches resulting from interconnected business processes or regulatory scrutiny, vendor risk management is getting a lot of attention at the highest levels of the organization. The numbers can be overwhelming as some organizations have thousands of vendors with access to corporate systems and technology in some way, shape or form. Clearly this isn't an issue that can be ignored any more.

We recommend a structure program for Vendor (IT) Risk Management that breaks partners up into risk tiers and figures out the level of oversight, assessment and reporting required for each tier. Technology is advancing rapidly that provides organizations with an ability to understand a vendor's security posture without requiring expensive site visits and penetration tests. Using this kind of intelligence allows organization's to assess their vendor's more frequently and focus efforts on those that are both critical and have serious security issues.

A critical aspect of defining the program is to ensure you have very clear plans for escalation and action in the event of an issue with a vendor. It will save you a lot of angst if business owners are very clear about the situations in which vendors will be quarantined or cut off. As with most things dealing with security, minimizing the amount of surprise to business owners and customers is a best practice.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com.

About the Analyst

Mike Rothman, Analyst and President

Mike’s bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business and brings a deep background in information security. After 20 years in and around security, he’s one of the guys who “knows where the bodies are buried” in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META’s initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.