# CYBER DEFENSE MAGAZINE

## eMAGAZINE

## APRIL 2021

# In This Edition

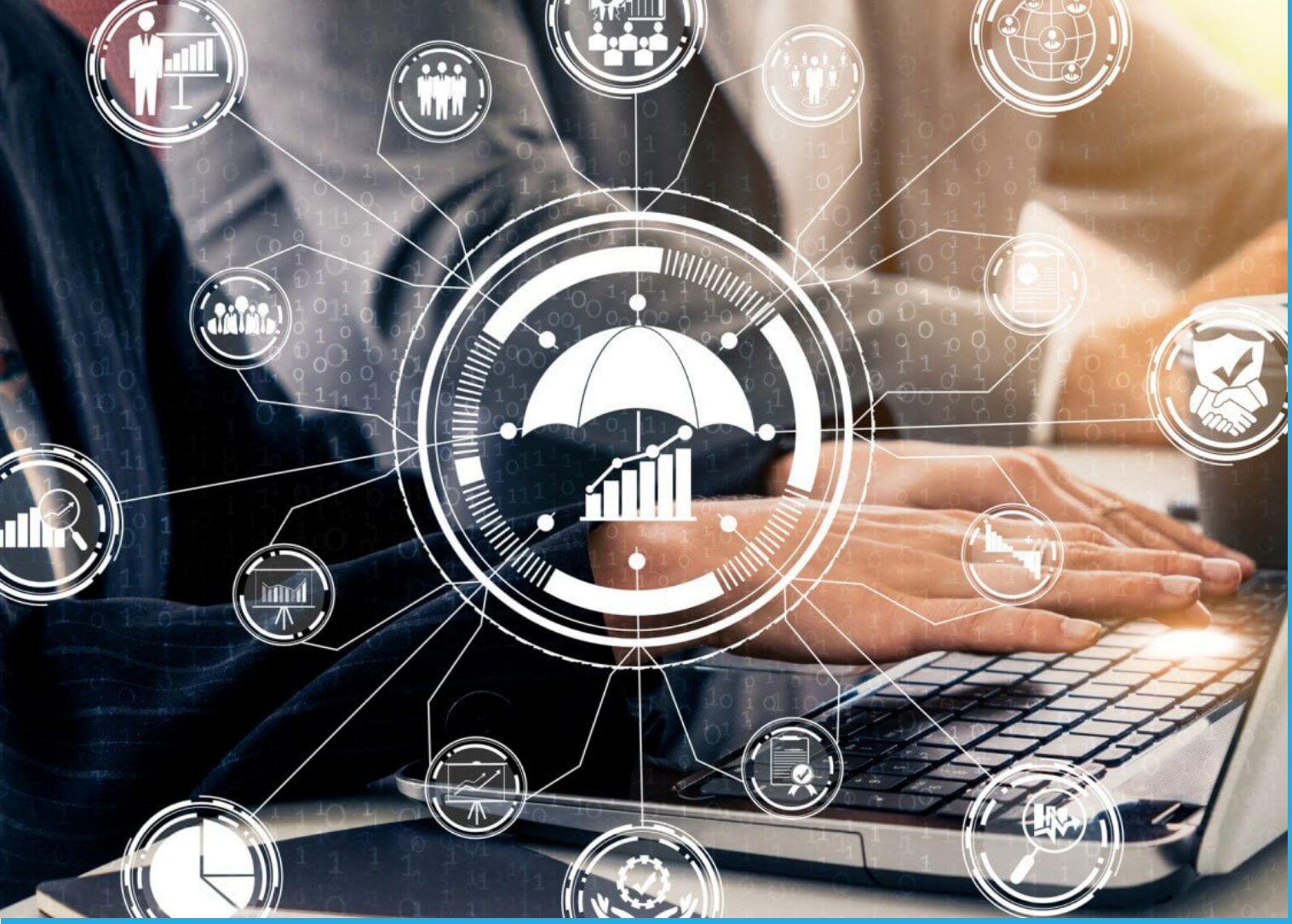

Cyber Defense 101 for 2021 and Beyond: The Case for Liberating Network Management

How Supply Chains Should Protect Themselves from Data Breaches

DevOps Done Right With Infrastructure-as-Code Security

Cybercrime Case in Detail


MORE INSIDE!



# Understanding the Risk of Supplier Management: A Six-Pronged Approach

**By Aaron Kiemele, Chief Information Security Officer at Jamf**

Years ago, I heard a story where thieves broke into a datacenter through the roof and lowered themselves, ninja-style, on cables. Seriously. Ninjas. On cables. Though rare, attacks such as this do, in fact, happen.

But far, far more likely? A nondescript person approaching the locked door, their arms full of boxes, asking for someone to let them into the office. Someone finding a dropped key and pocketing it. Someone figuring out that the side exit door never quite clicks shut unless someone leans hard on it.

This applies to cyberattacks as well. Some will be planned as a full-frontal assault from a nation-state type actor. But most? They'll sneak in through your weakest access point.

In the past, security professionals went by the old 'protecting us from ninjas' model. It was all about your perimeter. You had a firewall, a data center, all your secrets were locked behind concrete. It was all about guarding the doors and windows (and, perhaps, as in the previous rare case, the ceiling).

Much like a stealthy ninja, even the best and most robust security systems can neither detect nor protect against a fail on someone else's system or falls outside of the scope of the security system's capabilities. Consequently, the most common way to think about security is: where is your risk? How can you mitigate it?

Increasingly that risk is supplier management, exposing your business to the risk of a software vendor's vulnerability.

## Extent of the problem

Who outside of security professionals remember the details of how a company was breached? When it hits the news, everyone knows who got breached, but not much else. All breaches sound bad in a newspaper or blog post: they lose their customers' data and they lose their customers' trust. Did it really matter that the issue started with a third-party problem in a periphery device in a retail store or a vulnerability in a product without obvious direct access to data? It makes no difference. Their security failed. That is what people remember.

Often it failed because of a third-party integration, but that nuanced story is pointless. Not that they didn't make their own set of mistakes, but in most cases where there's a breach— even when it's terrible — security teams tried their best to do the right thing, and they fell to something on the margins.

And third-party breaches continue to dominate the headlines.

For instance, the SolarWinds breach [link: https://www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know/] almost certainly will go down as one of the biggest, most serious breaches in history.

The breach here wasn't a "hack" like in the movies; instead it was a seemingly valid patch to a great tool IT teams are using every day.

Their customers were now exposed through no fault of their own and now the companies themselves have to deal with the potential fallout and probable future attacks stemming from this leak.

The ultimate consequences of this vulnerability are still opaque, but at the very least attackers got privileged access into many global companies and government entities.

While there are innumerable causes for a security failure, the public sees it this way: if you fail, you fail. So how do you cover for this risk, and how do you reduce risk in the supply chain?

Turns out, that can be really tricky if you depend on only one way of doing things. You've got to have a multi-pronged approach.

## ONE: Vendor Screening

This type of risk has hardly been invisible. Many organizations have a Security Assurance Group: staff members who focus on answering supplier management questions for customers, to assure them the risk is manageable. Many companies require prescreening and for vendors to follow specific security protocols.

**Although this step can eliminate working with truly unsafe vendors, due diligence can go something like this:**

Q: Do you make terrible security mistakes?
A: We do not.
Q: Do you lock your doors?
A: We do.

There are varying degrees of vigor, but by and large, they're pretty straightforward. They can be an effective way of performing due diligence, but in the end, does vendor screening by itself get you to increased security? Can you be assured of your safety?

There is no single-threaded solution to risk; you need to do more.

Keep in mind that there is no perimeter anymore; we are all zero trust now whether we are prepared or not. It's important to note that risk cannot be eliminated. It's inherent in doing business and can only be mitigated. The question is this: what steps can organizations take to minimize risk from their third-party vendor pipeline? It's safe to assume that, even after doing your due diligence and vetting your supply chain, someone is going to be compromised. Assuming this to be true and covering all of your bases fully expecting such a compromise will put you in the best position.

## TWO: Balance of security and vulnerability

It's simply impossible to do business now without using multiple vendors expanding your risk profile dramatically. Everyone is doing their best to mitigate security issues with due diligence and supplier management processes, but the problem is that there are a million applications. All of them could have some sort of security issue and many could be in use in your environment.

Security is a business enablement function but my instinct is not immediately to support productivity as a singular goal.It's to reduce risk by finding a balance between productivity and risk. Know what your business needs to maximize its productivity and effectiveness, but also understand your tolerance for risk. What can the business accept and what can it not? This can form the basis for making informed decisions about supplier risk.

## THREE: Real risk mitigation is in the basics

Nobody is excited about this problem. There is absolutely no one announcing with pride their Computer Science major in Supplier Security Management.

So many people go into security thinking: "I'm gonna hack the planet and pen test everything," —and there is real value there— but often the best security is found in more mundane activities. Do I know what is in my vendors' change logs? How quickly can I evaluate and patch 100 applications . . . or a 1,000?

These are not exciting questions; they don't have an inherent sense of drama. But they are critical questions.

So what do you do, assuming that of your hundreds of vendors, at least some will have a breach in the next year?

**You focus on the fundamentals:**

- asset management
- identity and access management
- vendor due diligence and annual review
- robust and timely maintenance
- vigilance

## FOUR: You've got to see the problem

A central issue is visibility. How do we determine that an application has a patch available for a serious issue? There isn't necessarily a foolproof way to determine that at scale, but you have to do your best.

Most companies use the Common Vulnerability and Exposures (CVE) [link: https://cve.mitre.org/index.html] mechanism; this is a giant database governed by the public and private sector volunteers that lists all the vulnerabilities on most products.

But this depends on the company to be forthright about it. It's totally voluntary.

And companies can choose how to word the notices — some companies might be more interested in downplaying the issue than clearly explaining the problem, but in large part the data is good.

Though not comprehensive, it's one of the best tools we have, and regular scans of CVEs as well as regular reviews for patches in third party software will give you visibility into what existing, known problems you need to address.

Asset management is a security fundamental, you need to have a good sense of what happens on devices especially those where an employee has wide discretion to install applications without top down Security or IT involvement.

Chief among these are:

- what software is installed
- what services you use
- what you connect to (OneDrive, SharePoint, Dropbox, etc.)
- what does a "normal" system look like and how does it behave

Although this might not tell you exactly which vendor has a vulnerability, it will help you to keep an eye on entry points that are possible, and you can tighten up those entry points as much as possible by allowing only certain types of software, ensuring that where services interface with your own stack you've put some safeguards into place, and locking down those permissions as tightly as you can.

You need visibility into these questions: logs that are useful and sortable, an accurate inventory, and an awareness of the places you connect to others in your security framework.

And you need to have a strong focus not on an impenetrable security system (as we've shown, there is no longer any such thing), but on mitigating, rather than eliminating, risk. All you can do is drag the risk into the window that you can tolerate.

A good device management system with a strong inventory and permissions feature can help Security and IT sort through what happens in the event of a compromise of their internal systems after the fact, and push out a fix as quickly as possible.

## FIVE: Stick with Security 101

You do all the things you learn about in Security 101. You do them well. You do them consistently. You review, and you do them again.

**Can you answer these questions to your satisfaction?**

- Have you reviewed and ensured strong configuration management for your devices? You'll need a good MDM to stay on top of that.
- Can you effectively say who has access to what?
- What is your identity and access management solution, and what are its security vulnerabilities? State of your system
- Do you know everything that is running in your environment?
- Do you know what their patch status is?
- Do you know how many published vulnerabilities there are?
- Do you know what state individual workstations are in?
- Can you track this? Can you verify that it's correct?

## SIX: Consistent tracking and remediation, or: finding weird stuff

Effective endpoint security, effective monitoring and visibility and an effective system to set a response to patches can set you well on your way. Effective patching on a well-understood cadence based on this tracking is crucial.

If something weird happens, like 1500 logins for a user in a country you don't do business in, or from one dude in marketing (which is totally a true story), will you see it? Does your setup notice that sort of thing, and does it highlight things that are strange quickly?

Behavioral security doesn't just guard against known malware. It looks closely at activity, and at what is unusual or suspicious activity. What's weird, in whatever scenario? JavaScript running or programs downloading payloads in the middle of the night? Good behavioral endpoint protection identifies activity that acts like a virus or like a setup for malware, sandboxes it and reports it. In our current security climate, you can't really afford to not understand and measure for anomalous behavior.

## Mitigation, not lockdown

I'll say it again: there is no flashy — and certainly no easy — solution for dealing with the risks inherent in using third-party tools. It's all about covering your basics, doing due diligence and maintenance, and keeping your ear to the ground.

Following these best practices, maybe you can't say "I'm not vulnerable to anything today," but perhaps you can say with confidence "I'm not vulnerable to anything that came out last month." Or "I have 2020 on lockdown." If you can make it that far, and trust that if you have a well-planned process, you will be catching all sorts of problems before they even arise.

Remember: security should enable business, not throttle it. Drag your risk into a window you are comfortable with, and you'll be in a much better position to protect your system.
Even from ninjas.